(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 797 253**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.07.2017 E 17382493 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2020 EP 3435589**

(54) Título: **Un método y un sistema para encriptar comunicaciones inalámbricas que incluyen autenticación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2020

(73) Titular/es:

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

(72) Inventor/es:

GONZÁLEZ PÉREZ, PABLO;
TORRANO GIMÉNEZ, CARMEN y
ALONSO CEBRIÁN, JOSÉ MARÍA

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Un método y un sistema para encriptar comunicaciones inalámbricas que incluyen autenticación

Campo de la invención

La presente invención se refiere en general a conexiones inalámbricas. En particular, la presente invención se refiere a un método, y a un sistema, para encriptar comunicaciones inalámbricas que incluyen autenticación, particularmente usables para entornos de pequeña oficina/oficina doméstica (SOHO).

Se ha de indicar que la autenticación es el proceso de determinación de si alguien es, de hecho, quien ha declarado ser.

La biometría es la ciencia del establecimiento de la identidad de la persona basándose en atributos físicos o de comportamiento tales como la disposición o detalles específicos de las huellas dactilares, la cara, venas, oreja e iris, etc. Los sistemas biométricos están basados en la premisa de que los atributos físicos y de comportamiento pueden asociarse de manera inequívoca con un individuo.

La criptobiometría se refiere a la generación de claves de encriptación con biometría. Estos sistemas usan la biometría para crear claves, por lo tanto la autenticación está incluida implícitamente. Este paradigma reduce el inconveniente de recordar o llevar claves largas y complejas.

La contraseña de un solo uso basada en el tiempo (TOTP) es un algoritmo que genera dinámicamente claves únicas que se usan únicamente una vez introduciendo el tiempo actual para su cálculo. La TOTP se calcula usando una función de troceo que combina un componente fijo y uno dinámico, es decir, el secreto de TOTP (o la clave previamente compartida) y el tiempo actual. Se define en el documento RFC 6238. Aunque se usa el concepto de TOTP, la solución de la presente invención incluye algunas variaciones a la definición típica y/o implementación de TOTP.

Antecedentes de la invención

Los esquemas y protocolos para comunicaciones inalámbricas normalmente proporcionan una fase de asociación entre las partes de comunicación y una fase de transmisión. En la primera etapa se autentica el usuario.

Los sistemas de autenticación tradicionales que usan contraseñas para probar si el usuario es el correcto sufren de varias desventajas, tal como la suplantación en el caso de que la contraseña se robe o adivine. Los protocolos usados normalmente para asegurar redes inalámbricas, como WEP, WPA o WPA2 típicamente usan la clave previamente compartida para el cifrado de clave de la comunicación inalámbrica, que puede conducir a los problemas anteriormente mencionados.

Para evitar tales problemas y usar entradas de autenticación que sean más personales y puedan perfilar al usuario de manera inequívoca, existen algunos otros sistemas que usan características biométricas del usuario para autenticarle/la. La criptobiometría se refiere a la generación de claves de encriptación con biometría.

Además de eso, TOTP (contraseña de un solo uso basada en el tiempo) es un mecanismo que puede usarse para fortalecer la seguridad de sistemas puesto que incluye el tiempo actual y cambia periódicamente.

Además, la mayoría de los sistemas informáticos y de red existentes autentican un usuario únicamente en la sesión de inicio de sesión inicial. Las situaciones tales como compartición de dispositivo, robo de dispositivo o ataques de suplantación podrían conducir a situaciones de seguridad indeseables. La autenticación continua (mantener la usabilidad bajo términos aceptables) es necesaria para tratar este problema y monitorizar continuamente y autenticar el usuario que ha iniciado sesión para asegurar que él/ella es aún la persona que se espera que sea.

Existen algunas patentes o solicitudes de patentes conocidas en este campo.

El documento US-A1-20130004033 se refiere a un sistema de autenticación para autenticar al menos un objeto. El sistema de autenticación comprende: un dispositivo de captura para capturar al menos un registro de datos de salida biométricos para el objeto; un dispositivo de lectura para leer datos de configuración, asociados con el objeto, para una red neuronal artificial; un dispositivo de procesamiento que está diseñado para producir la red neuronal artificial y para introducir el registro de datos de salida biométricos en la red neuronal; un dispositivo de verificación que captura una salida desde la red neuronal para autenticar el objeto, en el que la red neuronal es una memoria asociativa bidireccional, particularmente una red de Hopfield, que tiene una multiplicidad de estados de red y el dispositivo de verificación está diseñado para determinar la salida de la red neuronal capturando un estado final derivado de la

entrada del registro de datos de salida biométricos. Un concepto fundamental de esta invención es el uso de una red neuronal para almacenar una clave asociada con una persona particular, en el que dicha clave se libera únicamente cuando se introducen datos biométricos apropiados en la red neuronal. A diferencia de la presente invención, esta invención no proporciona autenticación periódica.

El documento US-A1-20080113786 proporciona un dispositivo de juegos para identificar a un usuario, lo encripta y lo compara con el almacenado previamente en un dispositivo de autenticación. Se centra únicamente en autenticar al usuario. Aparte de la autenticación, la presente invención también incluye un método para cifrar/encriptar la comunicación inalámbrica e incluye autenticación periódica.

El documento US-A1-20110239276 está centrado en resolver la autorización en acceso inalámbrico creando un vector de característica con información de contexto y/o el estado del usuario y un perfil de usuario. El problema resuelto por esta solicitud de patente está más relacionado con la autorización de acceso a recursos de red asegurados. Por el contrario, la solución de la presente invención está más centrada en el problema de autenticación así como en cifrar la información intercambiada en la comunicación inalámbrica.

El documento WO-A1-2014141263 desvela un sistema para autenticación y autorización. El escenario implica uno o más clientes y un servidor de autenticación. El proceso es: el cliente genera una OTP, la encripta y genera credenciales de autenticación. El servidor desencripta la OTP del cliente y comprueba si coincide con la OTP generada por el servidor. En el caso de que las entradas biométricas de los clientes coincidan con los modelos biométricos, se genera la OTP. La solución de la presente invención, aparte de la autenticación, encripta la comunicación con una clave que contiene características biométricas del usuario, un factor aleatorio y uno temporal. De manera diferente a otros sistemas, las características biométricas se incluyen en el secreto de TOTP. Puesto que la clave de encriptación contiene las características biométricas en el secreto de TOTP, únicamente el usuario autorizado puede posibilitar la comunicación inalámbrica. Adicionalmente, la solución de la presente invención solicita el refresco de credenciales biométricas de manera periódica para verificar que el usuario es aún el que se autenticó.

El documento WO-A1-2016019127 desvela un sistema para autenticación con criptografía asimétrica. Para eso, existen tres elementos en la solución: un dispositivo de usuario, un dispositivo conectado y un servidor. El servidor envía un desafío cifrado con una clave pública al dispositivo conectado. El dispositivo conectado lo proporciona al dispositivo de usuario. El dispositivo de usuario descifra el desafío con una clave privada y genera un desafío convertido. El desafío convertido se envía al dispositivo conectado que lo proporciona al servidor de modo que puede validarlo y autenticar el usuario. El sistema podría usar también sensores biométricos para autenticación. Este sistema se centra únicamente en autenticar el usuario. Además de eso, la presente invención también incluye un método para cifrar/encriptar la comunicación inalámbrica e incluye autenticación periódica. El documento US-B2-8266681 desvela un método para proporcionar acceso a uno o más recursos en una red informática mediante un punto de acceso inalámbrico. El nivel de autorización del usuario se cambia dependiendo de los datos de autenticación recibidos desde el usuario. Un primer nivel de autenticación se asigna al dispositivo de cliente basándose en la autenticación. A continuación, se envía un programa al dispositivo de cliente, que está configurado de acuerdo con el guion de inicio de sesión. Después de ejecutar los programas, se envía la información del segundo nivel de autenticación en relación con el usuario del dispositivo. Si los segundos datos de autenticación son válidos, el segundo nivel de autenticación es mayor que el primero y comprende acceso a recursos de red adicionales. Si los segundos datos de autenticación no son válidos, el segundo nivel es más restringido y proporciona acceso a una subred del primero. Los datos de autenticación del dispositivo de cliente comprenden datos biométricos. Por lo tanto, esta solución se centra en la autenticación y autorización de un usuario para acceder a recursos a través de una red inalámbrica. Este sistema no usa OTP. De manera diferente de esta solución, la presente invención usa biometría para el secreto de TOTP. Además de autenticar el usuario, la solución de la presente invención proporciona autenticación periódica. También incluye un método para cifrar la comunicación con el punto de acceso y generar una clave de encriptación que únicamente permite que el usuario válido comunique en la red inalámbrica.

Se desvelan también soluciones adicionales en los documentos WO-A1-2015153559, US-A1-20160315771, US-A1-20020144128, US-A1-20120204245, US-A1-20120240204, US-A1-20170053252 y US-A-5229764.

Son por lo tanto necesarias más soluciones para asegurar que una comunicación inalámbrica se establece únicamente por la persona/usuario que se autenticó y que al mismo tiempo encripta la comunicación, que incluye información biométrica del usuario, y proporciona autenticación periódica para asegurar que dicho usuario está aún autorizado.

Descripción de la invención

Las realizaciones de la presente invención proporcionan, de acuerdo con un aspecto, un método para encriptar comunicaciones inalámbricas que incluyen autenticación, comprendiendo el método, inicialmente, establecer los parámetros de configuración para la conexión inalámbrica a una red de comunicación tal como Internet. Esto se hace

mediante un dispositivo de interconexión en red tal como un encaminador que recibe información de credenciales biométrica de un usuario (es decir, el usuario él/ella mismo/misma introduce su información biométrica tal como una huella dactilar, un reconocimiento facial, reconocimiento de voz, entre otros, en el dispositivo de interconexión en red), procesando la información de credenciales biométrica del usuario para extraer características biométricas de la misma, y generando un envío adicional a un dispositivo informático del usuario de una cadena aleatoria. El dispositivo de interconexión en red almacena las características biométricas extraídas y la cadena aleatoria generada en un registro del mismo.

A continuación, el dispositivo de interconexión en red recibe una solicitud para dicha conexión inalámbrica desde el dispositivo informático, y posteriormente el dispositivo informático recibe la información de credenciales biométrica desde el usuario que extrae características biométricas del mismo. A continuación, tanto el dispositivo informático como el dispositivo de interconexión en red generan un código de acceso temporal tal como una TOTP realizando una primera función criptográfica a través de la cadena aleatoria recibida/almacenada y las características biométricas que proporcionan un parámetro secreto y realizando una segunda función criptográfica a través del parámetro de secreto proporcionado y un parámetro de tiempo (es decir, un parámetro de tiempo que contiene el número de etapas de tiempo desde un contador inicial y el tiempo actual del dispositivo informático/dispositivo de interconexión en red). El dispositivo de interconexión en red almacena el código de acceso temporal generado en el registro. Debería observarse que para el funcionamiento correcto de la TOTP, los relojes de la red y del dispositivo informático necesitan estar sincronizados de manera aproximada.

A continuación, el dispositivo informático envía al dispositivo de interconexión en red una dirección de dispositivo del mismo, preferentemente su dirección de MAC, y un paquete de datos encriptados que contiene un texto dado, por ejemplo el texto ‘Hola’. El paquete de datos está encriptado con una clave de encriptación que corresponde al código de acceso temporal generado por el dispositivo informático. Cuando el dispositivo de interconexión en red recibe el texto encriptado, comprueba si la dirección de dispositivo recibida del dispositivo informático ya está almacenada en dicho registro. Pueden surgir dos situaciones en este punto, si dicha dirección de dispositivo no está almacenada en el registro (es decir, es una primera conexión del dispositivo informático), el dispositivo de interconexión en red comprueba cada clave de encriptación no asociada a una dirección de dispositivo hasta que halle la que desencripte y obtenga el texto dado, y actualiza dicho registro asociando la dirección del dispositivo al dispositivo informático, por el contrario, si dicha dirección de dispositivo se almacena en el registro, el dispositivo de interconexión en red usa la clave de encriptación asociada a la dirección del dispositivo para desencriptar el paquete de datos recibido. Finalmente, la conexión inalámbrica se establece entre el dispositivo informático y el dispositivo de interconexión en red, estando encriptada dicha conexión inalámbrica con la clave de encriptación.

Debería observarse que la conexión inalámbrica se establece únicamente si todos los factores (características biométricas, cadena aleatoria y factor temporal) coinciden con aquellos en el dispositivo de interconexión en red. Es decir, si en dicha primera conexión del dispositivo informático ninguna de las claves de encriptación no asociada a una dirección de dispositivo permite desencriptar el paquete de datos y obtener el texto dado, la conexión inalámbrica no se establece. Aparte, en las siguientes conexiones del dispositivo informático, si la clave asociada a la dirección del dispositivo no permite obtener el texto dado, la conexión inalámbrica no se establece tampoco.

De acuerdo con el método propuesto, el usuario se autentica cada cierto periodo de tiempo configurable por el dispositivo informático que solicita que el usuario reintroduzca la información de credenciales biométrica. En el caso de que la información de credenciales biométrica reintroducida no coincida con la almacenada en el registro el dispositivo de interconexión en red detiene la conexión inalámbrica. Además, los códigos de acceso temporales se generan periódicamente en un proceso paralelo y asíncrono a la conexión inalámbrica usando la cadena aleatoria, el parámetro de tiempo y la última información de credenciales biométrica introducida por el usuario en el dispositivo informático. En el caso del dispositivo de interconexión en red la información de credenciales biométrica se introdujo por el usuario en dicha etapa de ajuste. Puesto que el código de acceso temporal, usado para cifrar/encriptar la comunicación, cambia periódicamente, proporciona seguridad en el caso de que el código de acceso esté comprometido. Cada código de acceso es válido durante únicamente un cierto periodo de tiempo. Cada vez que el código de acceso temporal cambia, un paquete de datos con el texto dado se envía al dispositivo de interconexión en red, aparte de paquetes que corresponden a los datos de la comunicación, de modo que el dispositivo de interconexión en red puede comprobar si el texto obtenido en la desencriptación coincide con este texto, y a continuación se comprueban que los tres factores en el código de acceso temporal (biometría, cadena aleatoria, factor temporal) sean correctos. Si alguno de estos tres factores no son correctos, el dispositivo de interconexión en red detiene la conexión inalámbrica.

Preferentemente, el método propuesto se centra en las conexiones inalámbricas que tienen lugar en entornos de pequeña oficina/oficina doméstica (SOHO). Sin embargo, el método podría aplicarse también en un entorno empresarial, donde el usuario necesitaría acceder al encaminador de la compañía.

De acuerdo con una realización preferida, la primera función criptográfica comprende una función de troceo y la segunda función criptográfica comprende un código de autenticación de mensaje de troceo con clave (HMAC). En este caso, un cripto-parámetro de la segunda función criptográfica podría establecerse al algoritmo de troceo seguro de 512 bits en el que únicamente se toma la mitad de dichos bits y se usa la norma de encriptación avanzada (AES) como el algoritmo de encriptación para la clave de encriptación. Otra posibilidad sería usar el algoritmo de troceo seguro de 256 bits.

De acuerdo con una realización, la cadena aleatoria se envía al dispositivo informático mediante un código de respuesta rápida (QR).

Las realizaciones de la presente invención también proporcionan de acuerdo con otro aspecto un sistema para encriptar comunicaciones inalámbricas que incluyen autenticación que comprende un dispositivo informático y un dispositivo de interconexión en red para realizar las etapas y operaciones de realización del método anteriormente resumidas y desveladas en detalle a continuación. De acuerdo con el sistema propuesto el dispositivo informático tal como un teléfono móvil inteligente incluye uno o más procesadores y al menos una unidad biométrica configurada para recibir información de credenciales biométrica de un usuario, y el dispositivo de interconexión en red, que está configurado para proporcionar conexión inalámbrica a una red de comunicaciones a dicho dispositivo informático, incluye uno o más procesadores, una memoria y al menos una unidad biométrica configurada para recibir información de credenciales biométrica del usuario.

La presente invención proporciona un sistema criptobiométrico que identifica de manera inequívoca al usuario usando características biométricas del usuario. Además, la solución propuesta usa un factor aleatorio, un factor temporal y características biométricas para proteger la comunicación inalámbrica. Únicamente cuando todos estos tres elementos son correctos pueden establecerse las comunicaciones inalámbricas. Esto implica que la comunicación puede establecerse únicamente por la persona y el dispositivo que se autenticó. Además, proporciona autenticación (implícita) para una red inalámbrica.

El hecho de que la clave de encriptación de la comunicación cambie periódicamente proporciona seguridad para la comunicación en caso de que la clave se robara o comprometiera por cualquier razón.

Proporciona autenticación periódica para asegurar que el usuario es aún la persona autorizada. Puesto que las credenciales biométricas se solicitan periódicamente, es posible asegurar que el usuario del dispositivo es el que se autenticó.

La invención evita que cualquier otro usuario distinto al autorizado use la conexión inalámbrica (en el peor de los casos, la persona que suplanta podría usar la conexión únicamente hasta la siguiente vez que se soliciten de nuevo las credenciales biométricas). Esto es útil también en caso de robo del dispositivo informático del usuario.

Otra ventaja de la solución de la presente invención es que los visitantes en el escenario doméstico pueden conectarse a la red inalámbrica fácilmente, introduciendo sus credenciales biométricas en el dispositivo de interconexión en red. No es necesario proporcionales contraseñas largas. Aparte, es amigable para el usuario puesto que este proceso es transparente para el usuario.

Breve descripción de los dibujos

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

la figura 1 es un diagrama de secuencia que ilustra cómo se establecen los ajustes antes de la conexión inalámbrica entre el usuario y el dispositivo de interconexión en red.

La figura 2 es un diagrama de secuencia que ilustra cómo se genera la cadena aleatoria y se envía al dispositivo de usuario.

La figura 3 muestra esquemáticamente el proceso de generación periódica de las TOTP. Este proceso tiene lugar en paralelo y de manera asíncrona a los procesos de conexión/comunicación tanto en los dispositivos informáticos como de interconexión en red.

La figura 4 es un diagrama de secuencia que ilustra el proceso de la conexión inalámbrica realizado por el dispositivo informático de usuario.

La figura 5 es un diagrama de flujo que ilustra dos realizaciones diferentes realizadas por el dispositivo de interconexión en red después de que se recibe el paquete de datos con el texto encriptado.

Descripción detallada de la invención

La presente invención proporciona un método, y un sistema correspondiente, para encriptar comunicaciones inalámbricas que incluyen autenticación. Se supone que el dispositivo 20 de interconexión en red, tal como el encaminador, usado para proporcionar la conexión inalámbrica tiene capacidades (o medios o una unidad) para recibir entrada biométrica, tal como huella digital, reconocimiento facial o algún otro. El dispositivo 10 informático del usuario 1, tal como un dispositivo de teléfono inteligente o una tableta, entre otros, podría recibir también esa entrada biométrica. Adicionalmente, se supone que el dispositivo 20 de interconexión en red tiene capacidades para hacer algún procesamiento y almacenamiento. Estas capacidades podrían implementarse también en un servidor separado y servidor de autenticación si fuera necesario o adecuado.

La presente invención trata varios problemas al mismo tiempo. En primer lugar, la autenticación de un usuario en una red inalámbrica. Esto se proporciona usando biometría y es intrínseca a la solución. Aparte de autenticar el usuario, la solución propuesta proporciona encriptación y autenticación periódica. El método propuesto cifra la comunicación con el punto de acceso y genera una clave de encriptación que únicamente permite que el usuario válido comunique en la red inalámbrica. La comunicación se protege cambiando periódicamente la clave que cifra la información transmitida. Adicionalmente, puesto que la prueba biométrica se solicita periódicamente, es posible asegurar que el dispositivo 10 informático del usuario es el que inició sesión y no uno diferente. Por lo tanto, la seguridad de la propuesta radica en tres elementos: un factor aleatorio, uno temporal y uno biométrico. Únicamente la persona en posesión de estos tres elementos correctos al mismo tiempo puede conectar a la red inalámbrica.

La presente invención funciona como sigue. En una primera etapa, véase la figura 1, se establecen los ajustes para la comunicación inalámbrica. Para eso, el usuario 1 que desea usar la red inalámbrica introduce su información de credenciales biométrica en el dispositivo 20 de interconexión en red. Para eso, es necesario que el usuario 1 esté físicamente en el lugar donde está localizado el dispositivo 20 de interconexión en red. La información de credenciales biométrica puede recopilarse por diferentes mecanismos biométricos, tales como huellas dactilares, reconocimiento facial o cualquier otro mecanismo biométrico. Este proceso (establecimiento de los ajustes) tiene lugar únicamente una vez, antes de la primera vez que el usuario 1 desea acceder a la red inalámbrica. La información de credenciales biométrica se procesa y se extraen las características biométricas que caracterizan al usuario 1. Las características biométricas (o posiblemente un troceo de las mismas) se almacenan en un registro del dispositivo 20 de interconexión en red.

Después de eso, el dispositivo 20 de interconexión en red genera, véase la figura 2, una cadena aleatoria que se envía al dispositivo 10 informático preferentemente mediante un código de QR. El dispositivo 10 informático lee el QR y almacena la cadena aleatoria localmente. Aunque el QR es la implementación preferible, podría haber otros mecanismos para implementar la transmisión de esta información, tal como un SMS con un enlace universal que incluye la TOTP en la aplicación que controla.

Cuando el usuario 1 desea conectar a la red inalámbrica, el dispositivo 10 informático envía una solicitud para conexión al dispositivo 20 de interconexión en red. El dispositivo 20 de interconexión en red responde lanzando un desafío de autenticación, que solicita la información de credenciales biométrica. El usuario 1 introduce la información de credenciales biométrica en el dispositivo 10 informático (huella dactilar, reconocimiento facial u otro). Después de extraer las características biométricas de estas credenciales, los valores de estas características se almacenan. A continuación, se calcula un parámetro secreto del código de acceso temporal (es decir, una parte fija del código de acceso temporal, también denominado TOTP). Preferentemente, este se calcula realizando una primera función criptográfica tal como una función de troceo a través de las características biométricas extraídas y la cadena aleatoria, es decir, características biométricas concatenadas con la cadena aleatoria.

Siguiendo el documento RFC de TOTP, el código de acceso temporal final se calcula realizando una segunda función criptográfica a través de dicho parámetro secreto y un parámetro de tiempo. Una implementación posible para la segunda función criptográfica es usar SHA512 y tomar la mitad de los dígitos (256 bits). Obsérvese que en la presente invención, el valor de código de acceso temporal en esta solución contiene 256 bits y contiene caracteres alfanuméricos. Otras posibles implementaciones sería usar SHA-256 o SHA-3 de 256 bits.

Por lo tanto, se aplican dos funciones criptográficas para el cálculo del valor de código de acceso temporal: en primer lugar, para calcular el parámetro secreto con biometría y una cadena aleatoria. En segundo lugar para calcular el valor de código de acceso temporal para un cierto momento como se define en el documento RFC, es decir, aplicar una función HMAC que combina el parámetro secreto y el parámetro de tiempo actual (del dispositivo 10 informático y del dispositivo 20 de interconexión en red).

Puesto que el código de acceso temporal se genera periódicamente tanto por el dispositivo 10 informático como el dispositivo 20 de interconexión en red, se limita la cantidad de tiempo que una clave de encriptación es válida. A continuación, la clave que cifra la comunicación cambia periódicamente, lo que proporciona seguridad y robustez en caso de que la clave esté comprometida. El proceso de generación de TOTP tiene lugar en paralelo y de manera asíncrona a los procesos de conexión o de comunicación. La figura 3 representa el proceso de generación de códigos de acceso temporales tanto en el dispositivo 20 de interconexión en red como en el dispositivo 10 informático.

El dispositivo 20 de interconexión en red tiene un registro, o tabla, donde se almacena una tupla para cada dispositivo informático. La tupla contiene cuatro elementos: las características biométricas que identifican el usuario, la cadena aleatoria generada, el último código de acceso temporal generado (Kc), la dirección del dispositivo (preferentemente la dirección de MAC) del dispositivo 10 informático del usuario.

Volviendo al proceso de conexión, el dispositivo 10 informático encripta usando Kc como la clave de un paquete de datos especial que contiene un texto dado, tal como la palabra “Hola”. El valor de Kc corresponde al último código de acceso temporal generado (que varía periódicamente y depende de las características biométricas del usuario 1, un factor temporal y una cadena aleatoria). El dispositivo 10 informático envía el texto encriptado con Kc al dispositivo 20 de interconexión en red y la dirección del dispositivo del dispositivo 10 informático. Estas etapas se representan en la figura 4.

Cuando el dispositivo 20 de interconexión en red recibe el texto encriptado, comprueba (véase la figura 5) si la dirección del dispositivo del dispositivo 10 informático ya está registrada en el registro (etapa 500), es decir, si esa dirección de dispositivo está asociada a una clave de encriptación Kc, cadena aleatoria y características biométricas. La primera vez que un dispositivo 10 informático se conecta no está registrado, entonces el dispositivo 20 de interconexión en red intenta desencriptar el texto con todas las claves de encriptación Kc en el registro que no están asociadas a una dirección de dispositivo aún. Si el usuario 1 introdujo información de credenciales biométrica en la primera etapa (ajustes) y la cadena aleatoria en el dispositivo y factor temporal son correctos, hay una clave de encriptación Kc almacenada en el registro que puede desencriptar el texto y obtener como resultado el texto dado “Hola” (etapa 501). De hecho, el dispositivo 20 de interconexión en red puede distinguir la clave correcta puesto que en ese caso la desencriptación corresponde al texto dado “Hola”. Cuando se halla la clave de encriptación Kc, está asociada con la dirección del dispositivo del dispositivo 10 informático en el registro del dispositivo de interconexión en red (etapa 502). Ahora el dispositivo 20 de interconexión en red puede desencriptar con la clave de encriptación Kc (etapa 503).

Este proceso de búsqueda para la clave de encriptación Kc apropiada se hace únicamente la primera vez que un dispositivo 10 informático se conecta y se almacena para ocasiones siguientes. De manera contraria, si la dirección del dispositivo ya se registró en el registro, el dispositivo 20 de interconexión en red usa directamente la clave de encriptación Kc almacenada en el registro para desencriptar el paquete de datos recibido (etapa 503).

Después de estas etapas, se establece la comunicación inalámbrica y se encripta con la clave de encriptación Kc (que toma el valor del código de acceso temporal actual). Puesto que la clave de encriptación Kc depende de las características biométricas del usuario 1, únicamente esta persona puede establecer la comunicación inalámbrica. Adicionalmente, la comunicación puede establecerse únicamente si también los factores aleatorio y temporal son correctos. Esto evita casos de robo de dispositivos informáticos u otros usuarios que intentan usar la conexión del usuario legítimo 1. Una opción preferida y recomendada para implementar el algoritmo de encriptación es usar la norma actual (AES). Sin embargo, podrían incluirse otros algoritmos, por ejemplo, el algoritmo IDEA, entre otros.

Cada vez que cambia el código de acceso temporal, un paquete de datos con el texto dado se envía al dispositivo 20 de interconexión en red, aparte de paquetes que corresponden a datos de la comunicación, de modo que el dispositivo 20 de interconexión en red puede comprobar si el texto obtenido en la desencriptación coincide con este texto, y a continuación los tres factores en el código de acceso temporal (biometría, cadena aleatoria, factor temporal) se comprueban para que sean correctos. Si alguno de estos factores no son correctos, el dispositivo 20 de interconexión en red detiene la conexión inalámbrica.

Además de esto, la presente invención también incluye autenticación periódica. Esto se hace repitiendo el proceso ilustrado en la figura 4, excepto la solicitud de conexión (etapa 1). Significa que después de una cierta cantidad de tiempo, el dispositivo 10 informático solicita introducir información de credenciales biométrica de nuevo. Este intervalo de tiempo podría ser configurable por el dispositivo 20 de interconexión en red, dependiendo de los hábitos del usuario 1, por ejemplo, o por el usuario 1. En el proceso del cálculo de TOTP, el secreto de TOTP y el valor de TOTP se calculan con la nueva biometría introducida por el usuario 1. La TOTP se usa como la clave para cifrar el texto dado y se envía al dispositivo 20 de interconexión en red. Cuando el dispositivo 20 de interconexión en red lo recibe, desencripta el texto con la clave asociada a tal dirección de dispositivo (figura 5). Si la desencriptación obtiene el texto dado, la biometría era correcta y la conexión continúa sin interrupción. De otra manera se supone que el usuario 1 es

diferente y entonces no está autorizado. En este caso la comunicación inalámbrica se interrumpe.

La presente invención proporciona la autenticación del usuario 1 en la red inalámbrica. Adicionalmente, garantiza que el usuario 1 del dispositivo 10 informático sea el que inició sesión en el tiempo que dure la sesión. Las credenciales de autenticación identifican de manera inequívoca al usuario 1 puesto que se usa información de credenciales biométrica.

Además, aparte de la autenticación, la solución de la presente invención ofrece cifrar la comunicación con una clave que incluye características biométricas del usuario 1, un factor aleatorio y un factor temporal. Esto implica que únicamente el usuario autenticado pueda, aparte de autenticarse en la red inalámbrica, establecer comunicación con la red inalámbrica y hacer posible el intercambio de paquetes de datos que corresponden a la comunicación inalámbrica. Este nuevo enfoque establece un nuevo enfoque de seguridad para conectar a una red inalámbrica que puede observarse como una alternativa a otros protocolos de seguridad inalámbrica tales como WEP, WPA o WP2.

Aunque lo anterior se refiere a las realizaciones de la presente invención, pueden idearse otras realizaciones y adicionales de la invención sin alejarse del alcance básico de la misma. Por ejemplo, pueden implementarse otros aspectos en hardware o software o en una combinación de hardware y software.

Adicionalmente, los programas de software incluidos como parte de la invención pueden realizarse en un producto de programa informático que incluye un medio usable por ordenador. Por ejemplo, un medio usable por ordenador de este tipo puede incluir un dispositivo de memoria legible, tal como un dispositivo de disco duro, un dispositivo de memoria flash, un CD-ROM, un DVD/ROM o un disquete de ordenador, que tiene segmentos de código de programa legible por ordenador almacenados en el mismo. El medio legible por ordenador puede incluir también un enlace de comunicaciones, ya sea óptico, alámbrico o inalámbrico, que tiene segmentos de código de programa llevados en el mismo como señales digitales o analógicas.

El alcance de la presente invención se determina por las reivindicaciones que siguen.

REIVINDICACIONES

1. Método para encriptar comunicaciones inalámbricas que incluyen autenticación, que comprende:

a) establecer parámetros de configuración para que se establezca una conexión inalámbrica a una red de comunicaciones mediante un dispositivo (10) informático de un usuario (1) y un dispositivo (20) de interconexión en red, por el último (20):

recibir información de credenciales biométrica del usuario (1),

procesar la información de credenciales biométrica recibida, y

generar y enviar adicionalmente una cadena aleatoria a dicho dispositivo (10) informático, en el que las características biométricas extraídas desde dicha información de credenciales biométrica durante dicho procesamiento y la cadena aleatoria se almacenan en un registro del dispositivo (20) de interconexión en red;

b) recibir, por el dispositivo (20) de interconexión en red, una solicitud para la conexión inalámbrica a dicha red de comunicaciones desde el dispositivo (10) informático;

c) recibir, por el dispositivo (10) informático, la información de credenciales biométrica desde el usuario (1);

d) generar, por el dispositivo (10) informático y por el dispositivo (20) de interconexión en red, un código de acceso temporal,

en el que el dispositivo (10) informático que genera el código de acceso temporal realizando una primera función criptográfica a través de la cadena aleatoria recibida y las características biométricas extraídas desde dicha información de credenciales biométrica recibida que proporciona un parámetro secreto, y realizando una segunda función criptográfica a través de dicho parámetro secreto proporcionado y un parámetro de tiempo, en el que dicho parámetro de tiempo contiene el número de etapas de tiempo desde un contador inicial y el tiempo actual del dispositivo (10) informático,

en el que el dispositivo (20) de interconexión en red que genera el código de acceso temporal realizando una primera función criptográfica a través de la cadena aleatoria almacenada y las características biométricas extraídas desde la información de credenciales biométrica almacenada que proporciona un parámetro secreto, y realizando una segunda función criptográfica a través de dicho parámetro secreto proporcionado y un parámetro de tiempo, en el que dicho parámetro de tiempo contiene el número de etapas de tiempo desde un contador inicial y el tiempo actual del dispositivo (20) de interconexión en red, y en el que el dispositivo (20) de interconexión en red almacena su código de acceso temporal generado en dicho registro;

e) enviar, por el dispositivo (10) informático, al dispositivo (20) de interconexión en red, una dirección de dispositivo del dispositivo (10) informático y un paquete de datos encriptados que contiene un texto dado, encriptándose dicho paquete de datos con una clave de encriptación que corresponde al código de acceso temporal generado por el dispositivo (10) informático;

f) comprobar, por el dispositivo (20) de interconexión en red, si la dirección de dispositivo recibida del dispositivo (10) informático ya está almacenada en dicho registro, en el que:

si dicha dirección de dispositivo no está almacenada en el registro, el dispositivo (20) de interconexión en red comprueba cada clave de encriptación no asociada a una dirección de dispositivo hasta que halle la que desencripte y obtenga el texto dado, y actualiza dicho registro asociando la dirección del dispositivo al dispositivo (10) informático, o

si dicha dirección de dispositivo se almacena en el registro, el dispositivo (20) de interconexión en red usa la clave de encriptación asociada a la dirección del dispositivo para desencriptar el paquete de datos recibido; y

g) establecer la conexión inalámbrica entre el dispositivo (10) informático y el dispositivo (20) de interconexión en red, estando encriptada dicha conexión inalámbrica con la clave de encriptación,

en el que el usuario (1) que se autentica cada cierto periodo de tiempo configurable por el dispositivo (10) informático que solicita que el usuario (1) reintroduzca la información de credenciales biométrica, en el que si la información de credenciales biométrica reintroducida no coincide con la información de credenciales

biométrica recibida en la etapa a), el dispositivo (20) de interconexión en red detiene la conexión inalámbrica, y

en el que los códigos de acceso temporales en dicha etapa d) se generan periódicamente en un proceso paralelo y asíncrono a la conexión inalámbrica, generándose los códigos de acceso temporales usando la última información de credenciales biométrica introducida por el usuario (1) en el dispositivo (10) informático, por lo que cada vez que el código de acceso temporal cambia, se envía un paquete de datos con el texto dado al dispositivo (20) de interconexión en red, aparte de otros paquetes que corresponden a datos de la comunicación, de modo que el dispositivo (20) de interconexión en red puede comprobar si el texto obtenido en la desencriptación coincide con este texto, y a continuación se comprueban los tres factores, características biométricas, cadena aleatoria, parámetro de tiempo, en el código de acceso temporal para que se corrijan, deteniendo el dispositivo (20) de interconexión en red la conexión inalámbrica si alguno de estos factores no es correcto.

2. Método de la reivindicación 1, en el que la información de credenciales biométrica comprende al menos uno de una huella dactilar, reconocimiento facial o reconocimiento de voz.

3. Método de la reivindicación 1, en el que la primera función criptográfica comprende una función de troceo y la segunda función criptográfica comprende un código de autenticación de mensaje de troceo con clave, HMAC.

4. Método de la reivindicación 3, en el que un cripto-parámetro de la segunda función criptográfica se establece al algoritmo de troceo seguro de 512 bits en el que únicamente se toma la mitad de dichos bits y se usa la norma de encriptación avanzada, AES, como el algoritmo de encriptación para la clave de encriptación.

5. Método de la reivindicación 1, en el que dicho cierto periodo de tiempo configurable se establece por el dispositivo (20) de interconexión en red o por el usuario mediante el dispositivo (10) informático.

6. Método de la reivindicación 1, en el que la cadena aleatoria se envía al dispositivo (10) informático mediante un código de respuesta rápida, QR.

7. Sistema para encriptar comunicaciones inalámbricas que incluyen autenticación, que comprende:

un dispositivo (10) informático que incluye uno o más procesadores, una memoria y al menos una unidad biométrica configurada para recibir información de credenciales biométrica de un usuario (1); y

un dispositivo (20) de interconexión en red configurado para proporcionar conexión inalámbrica a una red de comunicaciones a dicho dispositivo (10) informático, incluyendo el dispositivo (10) de interconexión en red uno o más procesadores, una memoria y al menos una unidad biométrica configurada para recibir información de credenciales biométrica desde el usuario (1),

en el que el dispositivo (10) informático y el dispositivo (20) de interconexión en red están configurados para implementar el método de una cualquiera de las reivindicaciones 1 a 6.

8. Sistema de la reivindicación 7, en el que el dispositivo (10) informático comprende al menos un dispositivo de teléfono móvil inteligente, una tableta, un ordenador o un portátil.

9. Sistema de la reivindicación 7, en el que el dispositivo (20) de interconexión en red comprende un encaminador.

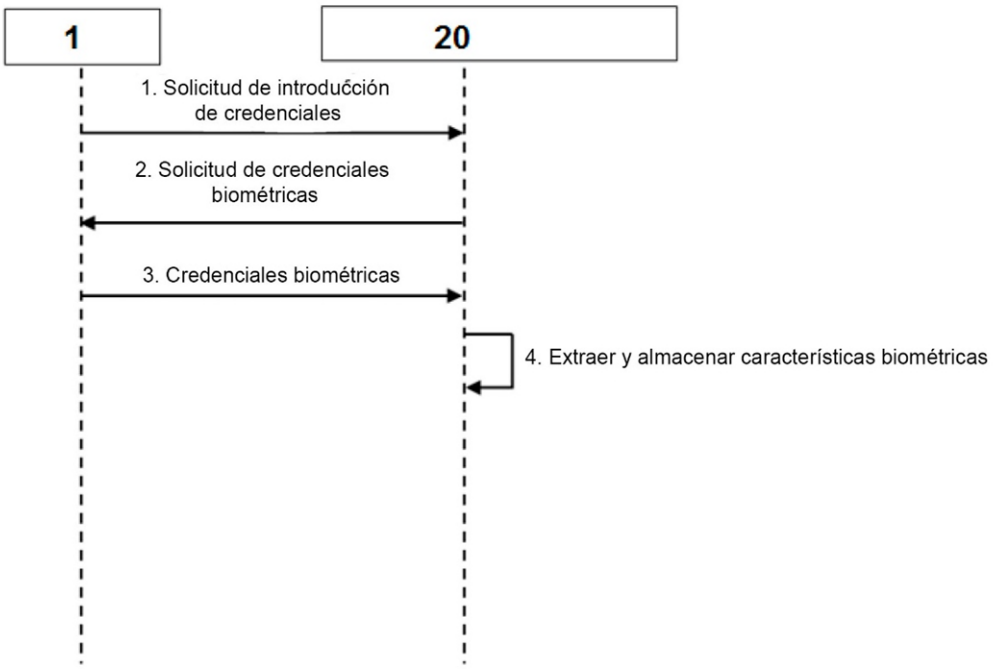
1
20
1. Solicitud de introducción de credenciales
2. Solicitud de credenciales biométricas
3. Credenciales biométricas
4. Extraer y almacenar características biométricas

Fig. 1

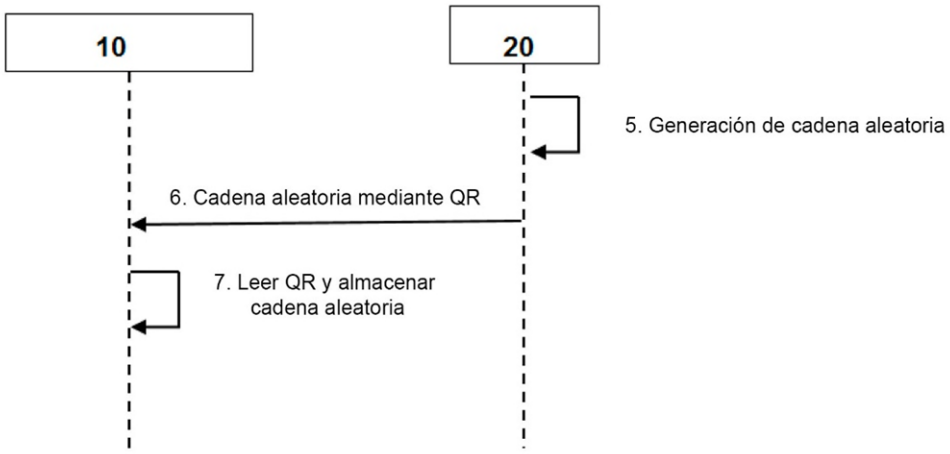
10
20
5. Generación de cadena aleatoria
6. Cadena aleatoria mediante QR
7. Leer QR y almacenar cadena aleatoria

Fig. 2

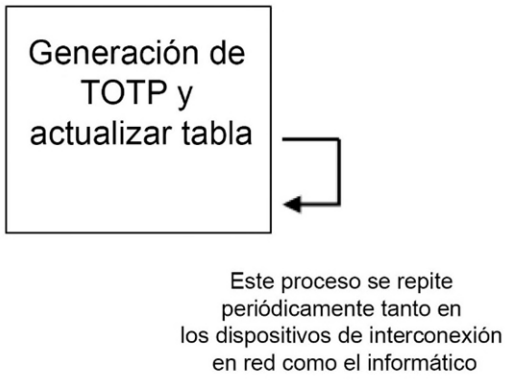
Generación de TOTP y actualizar tabla
Este proceso se repite periódicamente tanto en los dispositivos de interconexión en red como el informático

Fig. 3

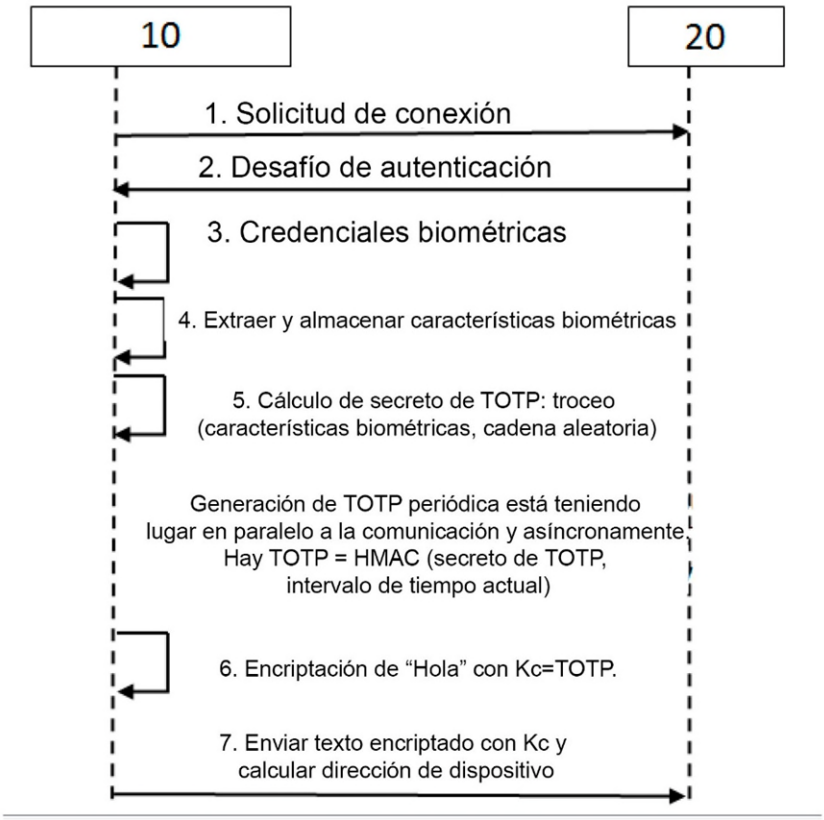
10
20
1. Solicitud de conexión
2. Desafío de autenticación
3. Credenciales biométricas
4. Extraer y almacenar características biométricas
5. Cálculo de secreto de TOTP: troceo (características biométricas, cadena aleatoria)
Generación de TOTP periódica está teniendo lugar en paralelo a la comunicación y asíncronamente. Hay TOTP = HMAC (secreto de TOTP, intervalo de tiempo actual)
6. Encriptación de “Hola” con Kc=TOTP.
7. Enviar texto encriptado con Kc y calcular dirección de dispositivo

Fig. 4

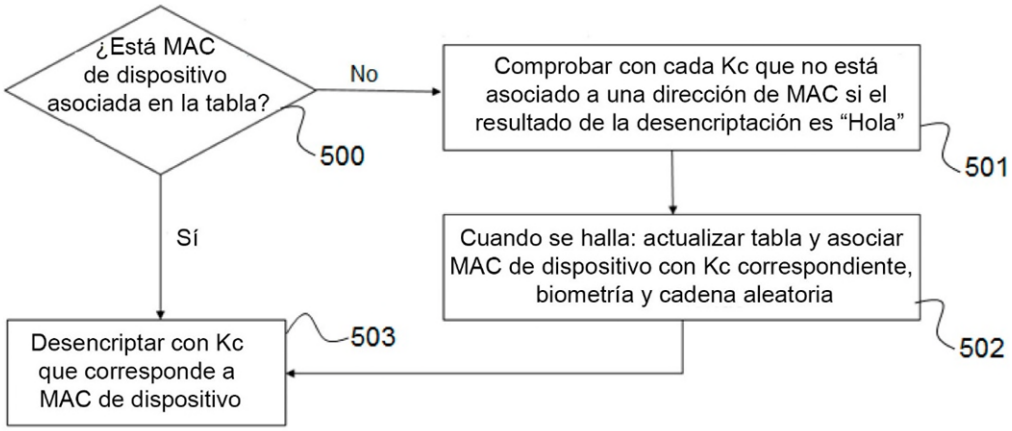
¿Está MAC de dispositivo asociada en la tabla?
500
No
Sí
Comprobar con cada Kc que no está asociado a una dirección de MAC si el resultado de la desencriptación es “Hola”
501
Cuando se halla: actualizar tabla y asociar MAC de dispositivo con Kc correspondiente, biometría y cadena aleatoria
502
Desencriptar con Kc que corresponde a MAC de dispositivo
503

Fig. 5