(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 663 390**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/30 (2013.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.03.2013 PCT/US2013/032405**

(87) Fecha y número de publicación internacional: **03.04.2014 WO14051695**

(96) Fecha de presentación y número de la solicitud europea: **15.03.2013 E 13842480 (9)**

(97) Fecha y número de publicación de la concesión europea: **28.02.2018 EP 2901616**

(54) Título: **Método para la autenticación de contexto de seguridad móvil**

(30) Prioridad:

28.09.2012 US 201261707190 P
14.03.2013 US 201313803796

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.04.2018

(73) Titular/es:

HESSLER, CHRISTIAN J. (100.0%)
10343 Federal Blvd J 409
Westminster CO 80260, US

(72) Inventor/es:

HESSLER, CHRISTIAN J.

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método para la autenticación de contexto de seguridad móvil

Referencia cruzada a solicitudes relacionadas

Esta solicitud tiene prioridad de la solicitud de patente provisional de los Estados Unidos núm. 61/707,190, presentada el 28 de septiembre de 2012, titulada "Mobile Security Context Authentication," por el inventor Christian J. Hessler, cuyos contenidos se incorporan expresamente en la presente descripción mediante esta referencia.

Campo de la invención

La presente invención se refiere generalmente a un método y sistema para proporcionar seguridad y autenticación de red. En particular, la invención se refiere a sistemas y métodos de seguridad de autenticación de contexto de múltiples factores que usan un dispositivo informático electrónico móvil a través de una red que usa factores contextuales dentro de una sesión definida.

Antecedentes de la invención

Durante décadas, varios usuarios de ordenadores generalmente han usado esquemas de autenticación basados en contraseña o PIN. Estos métodos generalmente se realizan a través de un acceso de usuario tradicional desde un dispositivo informático electrónico fijo o móvil. El usuario generalmente usa un dispositivo informático electrónico móvil, tal como un ordenador de escritorio, un ordenador portátil, una tableta, un ordenador móvil o teléfono, o teléfono inteligente, para acceder a un recurso particular, interno o externo, tal como un sitio web, una aplicación, un servidor, o una red. Al acceder al recurso particular mediante el uso de los medios tradicionales, el usuario típicamente ingresa un nombre de usuario y una contraseña para autenticarse y puede usar algún método de verificación adicional tal como un mensaje fuera de banda, secreto compartido, ficha física, certificado o protocolo de comunicación de campo cercano.

El acceso de usuario tradicional se ha usado además en otras áreas, tal como el área de transacciones de pago. Cuando un usuario desea realizar una transacción de pago, el usuario a menudo se enfrenta con un esquema de verificación en el que el usuario utiliza algún nivel de privilegio o autorización del pago. Aunque el ámbito de pago es un área que ha sido muy popular para las áreas de privilegio o autorización, el esquema de autenticación no se limita a los pagos, ya que puede usarse en otras áreas, tal como el acceso a un activo en particular. En cualquier caso, el proceso de autorización típicamente requiere el uso de cualquiera de los siguientes: un dispositivo informático, una sesión, un sitio web, una aplicación, un servidor, una ubicación y/o un recurso.

Desafortunadamente, la mayoría de los métodos de autenticación tradicionales tienen varios defectos y complicaciones. Por ejemplo, muchos métodos de autenticación convencionales son o demasiado costosos o demasiado engorrosos para escalar apropiadamente y adoptarse de forma ubicua por el mercado. Adicionalmente, los métodos y sistemas de autenticación actuales no están a la altura del desafío de seguridad que representan los hackers modernos y no tienen las características de facilidad de uso o privacidad que los usuarios requieren. Además, las soluciones contemporáneas de múltiples factores o de dos factores no reconocen ni explotan el hecho de que la seguridad del usuario es un tejido, no un hilo conductor - *es decir*, compuesto de múltiples variables, en lugar de, un solo factor o variable. Esta ignorancia de las realidades contextuales entre dispositivos, sitios, usuarios, aplicaciones y redes en entornos empresariales y sociales hace que la mayoría de las soluciones sean deplorablemente inadecuadas para cumplir con los desafíos de seguridad de autenticación disponibles.

Aunque los métodos adicionales pueden intentar abordar estos problemas colapsando los actos de identificación y autenticación en un solo proceso, estos métodos heredan las mismas responsabilidades que cualquier otro punto único de fallo o sistemas federados, independientemente de la sofisticación o novedad del flujo. El desafío siempre ha sido equilibrar la seguridad avanzada con una facilidad de uso mejorada.

De forma innovadora, el método de autenticación que cumpliría las necesidades de los procesos y demandas de verificación actuales sería usar múltiples capas de credenciales o factores contextuales. Los ejemplos de tales factores incluirían información sobre: un servidor o servicio, una red, un usuario en un dispositivo fijo o móvil, una ubicación, una proximidad física y digital, una relación o asociación, factores sintetizados/holísticos (frente a secuenciales o aislados), y comportamientos o atributos de alguno o todos los anteriores. Preferentemente, el proceso ideal de autenticación se usaría en un entorno de sesión o transacción de alto valor/bajo volumen, tal como actividades bancarias, datos de atención médica, el ejército, o un contexto legal. El proceso de autenticación podría usarse además en un espacio de bajo valor/alto volumen, tal como el comercio electrónico, las redes sociales o los juegos. Además, la estructura del proceso de autenticación ideal e innovador debería ser adaptable para la arquitectura de cliente a servidor, de servidor a servidor, de igual a igual o híbrida. La expectativa de, y el requisito para, la privacidad, la facilidad de uso, la precisión, la simplicidad, y la solidez son preferentemente equivalentes en todos los escenarios.

El desafío, sin embargo, es crear una verificación contextual simple y mutua sin depender de o exponer el proceso a los defectos de las soluciones de seguridad tradicionales. Dichos defectos incluyen, pero no se limitan a, cuestiones

relacionadas con: el costo, la persistencia, la falta de privacidad, la interceptación, la repetición, la facilidad de uso, la dependencia de las habilidades del usuario, la encriptación, la ofuscación, la siembra de información, la presentación o envío combinado y/o transmisión de las credenciales reutilizadas a través de canales conocidos o predecibles, la inspección y evaluación secuencial y discreta de credenciales aisladas, y la toma de decisiones autoritaria unilateral sobre el estado del resultado del contexto. Debido a que los medios convencionales de autenticación incluyen el emparejamiento de elementos discretos y privados de un usuario, dispositivo, o sesión con sus significados (pares clave-valor), estos métodos colapsan indebidamente las nociones independientes de identificación (autorreportada) y autenticación (verificadas externamente). Como resultado, la información privada de la identidad del usuario se expone potencialmente a la captura, reproducción, predicción, robo o uso indebido, en servicio de su verificación.

Un segundo desafío para crear un método de autenticación ideal e innovador es utilizar el dispositivo móvil en un contexto de seguridad para el que se diseña y es capaz de: ser una extensión interactiva de y participante dentro del contexto de autenticación del usuario, sitio/aplicación y sesión. Las encarnaciones anteriores de "traiga su propio dispositivo" o los métodos de autenticación de dispositivos móviles trataban al dispositivo informático móvil simplemente como un aparato de "captura y reenvío". El dispositivo generalmente se usa para capturar, decodificar y reenviar las credenciales, claves o fichas, en lugar de participar de una manera en la que es capaz. Específicamente, las invenciones anteriores simplemente relegaban el dispositivo móvil para ser una cámara y un disco duro, almacenar claves ofuscadas o cookies y reenviarlas a lo largo del servidor autoritario de extremo posterior para una búsqueda de contraseña estándar y un enfoque de coincidencia. Sin embargo, el uso de un dispositivo móvil como parte del esquema de autenticación fortalecerá el proceso de verificación al añadir "autenticación de realidad aumentada"-es decir, usar el dispositivo móvil para interactuar con el tejido del usuario, el entorno, la ubicación, la proximidad, el comportamiento y el contexto de la sesión de una manera que revoluciona de manera segura, privada y fácil el proceso de autenticación tradicional.

Una tercera oportunidad es involucrar al usuario en el proceso de autenticación de una manera única que nunca se ha logrado con los métodos de autenticación convencionales. Las soluciones de seguridad anteriores se consideraban como una o más capas o etapas engorrosas en el flujo de seguridad del usuario final. Los usuarios tenían que, por ejemplo, responder a ciertos desafíos de contraseñas o mantener la custodia de credenciales de hardware o software personalizadas tales como fichas, claves, certificados o seleccionar componentes visuales, audibles, matemáticos o textuales reconocibles a partir de una serie de interfaces y mensajes. El usuario simplemente nunca ha participado en las credenciales o el proceso de autenticación, sino que simplemente ha sido responsable de responder a esos componentes o etapas a petición del sitio web del sistema central o la aplicación. Debido a que un sitio web generalmente contiene todas las claves de accesibilidad de seguridad, la piratería del lado del usuario (*p. ej*., los registradores de digitación, el hombre en el medio, el hombre en el navegador, phishing, pharming, whaling, la ingeniería social y otras técnicas similares) ha aumentado y ha dado como resultado un cambio necesario desde la vista del lado del sistema central-servidor de la seguridad de autenticación a un enfoque más interactivo y centrado en el usuario. El usuario debe tener un control interactivo de la profundidad, la manera, el método, la construcción y la personalización de su seguridad de autenticación que sea más sólido, contextual y más efectivo que las técnicas anteriores. Adicionalmente, el método de autenticación ideal debería ser además más simple, más elegante y altamente utilizable.

Estos desafíos, en resumen, han representado una barrera para aquellos que buscan soluciones y nunca han sido superados por los métodos convencionales. Dado que no existe, y que nunca ha habido un enfoque único, exitoso y ubicuo para la autenticación interactiva de usuarios en el campo, habla mucho de las deficiencias de los métodos e implementaciones convencionales. Como resultado, no se ha adoptado de hecho una técnica en el campo de la autenticación de múltiples factores de usuario final que resuelva simultáneamente los desafíos de seguridad, facilidad de uso e interactividad establecidos en la presente descripción.

El objetivo o solución sería crear un proceso, sistema o método de autenticación que utilizaría la verificación del contexto y la autenticación de todas las partes y factores, al tiempo que permanecería inmune a varios problemas de autenticación (*p. ej.* amenazas, piratería, intercepción, repetición, compromiso, predicción, colusión, resultados falsos o cualquiera del proceso, método, responsabilidades de implementación). Además, el proceso de autenticación abarcaría la facilidad de uso, alcanzaría la ubicuidad potencial con la integración de baja tecnología o sin tecnología, y elevaría el dispositivo móvil a un miembro interactivo del algoritmo de autenticación. Esto proporcionaría preferentemente al usuario un control adicional y personal sobre su seguridad a través de factores de ubicación/comportamiento/personalización "realizados", que están más allá de la profundidad o los requisitos de la credencial de seguridad nativa. A diferencia de la técnica anterior en este espacio que intentaba "identificar" un usuario por su comportamiento o ubicación personalizada, tal como el seguimiento GPS, la medición biométrica, la medición de pulsaciones, el reconocimiento facial o de voz, la nueva solución lograría la autenticación de contexto de estos factores compuestos por la naturaleza de su presente e influencia en la decisión, sin revelar o seguir de forma inapropiada la identidad personal inmutable del usuario a través de su captura, inspección, aplicación y/o interrogatorio literal.

Existen varias referencias que describen los métodos de autenticación que utilizan un dispositivo y una red. Por ejemplo, la publicación de la solicitud de Patente de los Estados Unidos núm. 2011/0219427, presentada por Hito y otros (en lo sucesivo "Hito"), y la publicación de la solicitud de Patente del Reino Unido núm. W2012/069845, presentada por Harris (en lo sucesivo "Harris"), describen diversos métodos de autenticación y codificación. Específicamente, la referencia de

Hito describe técnicas para simplificar un proceso de autenticación desde el punto de vista del usuario mientras se emplea una seguridad mejorada para otro usuario que emplea técnicas de seguridad débiles o inexistentes. En lugar de usar el nombre de usuario y la contraseña convencionales, el método de autenticación descrito en Hito utiliza una señal codificada, que se comunica desde un teléfono inteligente hasta un servidor de autenticación. La señal codificada informa al servidor si el usuario se ha autenticado correctamente o no. Aunque Hito describe técnicas de verificación y autenticación que van más allá del esquema tradicional de nombre de usuario/contraseña, Hito no utiliza factores contextuales en una sesión de usuario definida (p. ej., factores de comportamiento, factores de ubicación, factores de personalización) que ayudarían a fortalecer el proceso de verificación.

Con respecto a la publicación de la solicitud de patente del Reino Unido núm. W2012/069845 presentada por Harris, la referencia de Harris describe un método de autenticación que utiliza un dispositivo portátil, un primer servidor y un segundo servidor. El dispositivo portátil obtiene información codificada y decodifica la información. Después de decodificar la información, el dispositivo portátil transmite un mensaje al primer servidor; en donde el primer servidor incluye la información decodificada y un primer identificador, que identifica el dispositivo o el usuario. El primer servidor recibe el mensaje y establece la identidad del usuario o dispositivo. Como resultado, el primer servidor realiza una acción basada en la información decodificada. La referencia de Harris puede usar además otros diversos factores de autenticación, tales como la posesión del dispositivo y el conocimiento de una contraseña. Sin embargo, al igual que la referencia de Hito, Harris no utiliza factores contextuales basados en una sesión de usuario definida que fortalecería el proceso de verificación.

Ambos casos de las referencias citadas anteriormente se basan en el enfoque común de sembrar las credenciales dentro de los mensajes de sesión, transmitirlas como pares clave-valor de forma unidireccional para verificase por una única fuente autoritaria que establece esa autenticidad mediante el almacenamiento en el servidor, recuperación y coincidencia de los factores literales. Además, la autoridad del servidor debe capturar, almacenar y referenciar el conocimiento literal compartido y reutilizado sobre el usuario, el sitio, el dispositivo y los identificadores de sesión durante la comparación, que puede usarse, fuera de contexto, para reconstruir o reproducir una sesión de autenticación existente válida. La custodia y confidencialidad de estos identificadores estáticos durante la captura, el almacenamiento o la transmisión es la clave de la eficacia de la técnica anterior, independientemente de la novedad de la presentación o transmisión. Es esta incapacidad para innovar más allá de esta convención la que soporta la mayoría de las infracciones, pirateos y fallos que plagan los métodos de autenticación actuales, que incluyen estos, en la práctica en la actualidad. Sin lograr un tratamiento dinámico y sensible al contexto de los factores de autenticación no identificables mutuamente afirmados en un marco triangulado (versus unidireccional), no puede existir innovación más allá de lo convencional, ni una solución inventiva viable a los fallos de la técnica anterior.

Además de las dos referencias enumeradas anteriormente, existen muchas referencias relevantes dentro del campo de la presente invención. Sin embargo, estas referencias tienden además a caer en un conjunto definible de enfoques inadecuados, que se remontan a nociones de seguridad anticuadas desde principios hasta mediados del siglo XX. El advenimiento de la tecnología móvil ha desatado una serie de nuevas técnicas y referencias que utilizan las capacidades de detección, procesamiento y transmisión móvil de los dispositivos informáticos móviles. Desafortunadamente, estas referencias incorporan las capacidades multipropósito dentro de los paradigmas de autenticación obsoletos, los modelos de secreto compartido, la seguridad mediante el procesamiento unidireccional no sensible al contexto, anónimo y plano, independientemente de sus características fuera de banda (OOB) o flujo.

Estas referencias relevantes se han basado en cuatro modos principales de autenticación por encima del nombre de usuario/contraseña o el inicio de sesión único (SSO): (1) sembrar y leer (almacenar la credencial en el dispositivo y la referencia tras la autenticación posterior); (2) buscar y coincidir (reconocimiento de navegador/dispositivo dinámico basado en escritura, cookies); (3) llamar y hacer ping (fuera de banda, contraseñas o fichas de un solo uso, secretos compartidos, PIN); y (4) decodificar y reenviar (modelo basado en código QR para capturar el código, hacerlo coincidir con la credencial sembrada y reenviarlo al servidor de extremo posterior para la búsqueda y coincidencia)

Específicamente, las deficiencias de las referencias enumeradas anteriormente se incluyen en estas áreas: (1) facilidad de uso engorrosa para el usuario final; (2) proceso de inscripción del usuario que expone el enlace de confianza inicial más débil; (3) falta de integridad de credenciales a través de afirmaciones de múltiples perspectivas; (4) falta de conocimiento de la ubicación, proximidad, historial o movimiento de la credencial, el usuario o el dispositivo; (5) disminución de la privacidad del usuario a través de la repetición de la transmisión por pares de identificadores estáticos; (6) falta de flexibilidad o diversidad de credenciales; (7) fallo para lograr la ubicuidad en todos los tipos de dispositivos y sesiones; (8) flujo incorrecto de credenciales (de un canal seguro a uno inseguro); (9) autoridad de afirmación unilateral (proceso de búsqueda/coincidencia único); (10) falta de conocimiento del contexto de credenciales (tiempo, ubicación, comportamiento); (11) falta de control del usuario sobre la profundidad, composición y proceso de la credencial; (12) sobreidentificación del usuario o dispositivo durante la autenticación; (13) transmisión innecesaria de pares de valores claves de datos de identificación de usuario o dispositivo; (14) componentes pesados tales como PKI (encriptación de clave pública/privada), certificados digitales y claves permanentes que requieren administración de distribución, ofuscación y revocación en el dispositivo móvil; (15) flujo unidireccional de credenciales de clave-valor hacia un único objetivo autoritario; (16) perspectiva única o medida de las credenciales de contexto; y (17) relegación no interactiva del dispositivo inteligente a una simple utilidad de decodificación y reenvío.

Varias modalidades descritas previamente no han podido resolver adecuadamente las necesidades de seguridad actuales, como se evidencia por los ataques de seguridad en curso realizados con éxito por hackers y delincuentes. Además, las soluciones propuestas por las soluciones de seguridad actuales no resuelven los siguientes problemas, específicamente: (a) la autenticación se comparte tradicionalmente como secreta, estática y sujeta a la intercepción, repetición o predicción basada en la información persistente sólo ofuscada por la encriptación o aromatización de la sesión; (b) la seguridad de autenticación es costosa, engorrosa, difícil de entender o usar por los usuarios; (c) la autenticación se basa en la ofuscación, la encriptación, la habilidad/custodia del usuario o el secreto para ser efectiva; (d) las credenciales normalmente son fijas, secuenciales y de una sola masa en profundidad, inteligencia y contexto; (e) la información de seguridad fluye hacia atrás, sobre los canales primarios, predictivos o conocidos, tal como el navegador, juntos como pares clave-valor, hacia la autoridad unilateral en el proceso; (f) la decisión de autenticación se basa en una observación, interrogación, búsqueda de coincidencia unilateral o una afirmación autoritaria simple de credenciales, normalmente en una relación patriarcal cliente-servidor entre el identificador y el que se identifica. La autenticación mutua es una idea de último momento; (g) la información de seguridad secreta a menudo se entrega a través de canales fuera de banda seguros (OOB), sólo para que el usuario o dispositivo vuelva a insertar ese secreto aún no verificado nuevamente en el canal no seguro principal (*p. ej.*, el navegador); (h) el usuario asume todos los riesgos/responsabilidades, pero no tiene control sobre el incremento, modificación o mejora de su seguridad más allá de lo que la fuente emisora/autoritaria requiere o permite; (i) la seguridad requiere una nueva identificación o el usuario o dispositivo junto con la autenticación, mezclando las credenciales en el canal; (j) la seguridad de la autenticación es arriesgada cuando se utiliza con un dispositivo móvil cuya integridad es desconocida; (k) hasta la fecha, no ha habido una invención ubicua para aplicar la autenticación de defensa en profundidad además del inicio de sesión único en la parte superior del nombre de usuario/contraseña, el inicio de sesión único (SSO) o el enfoque de gestión de identidades; (l) la seguridad que se basa en la ubicación sólo mide la interpretación digital de ese lugar, y no puede triangular lo físico (línea de visión, línea de sonido, línea de sensación) con lo digital; (m) la verdadera defensa en profundidad, una capa de autenticación adecuada de una especie diferente a la identificación autoinformada inicial, a menudo se ignora en vez de simplemente contraseñas o secretos adicionales, o la suposición de que la identidad por referencia (es decir, SSO) es adecuada para la categoría de autenticación; y (n) los enfoques basados en plantillas simplemente han sido contenedores estáticos para la recopilación tradicional de factores literales y la transmisión unidireccional de vuelta a un único almacenamiento de datos autoritario para una comparación no contextual aislada.

Específicamente, las soluciones propuestas en la lista de referencias anterior que usan imágenes codificadas de respuesta rápida (QR) y el escaneo de dispositivos móviles para identificar o autenticar a un usuario o dispositivo, como la referencia de Hito y similares, son insuficientes debido a las siguientes limitaciones y métodos inferiores: (a) la confianza en el contenido fuertemente codificado, encriptado u ofuscado dentro de la imagen o código QR en sí, tal como un servidor web, usuario, dispositivo, identidad o información de sesión - y la integridad y confidencialidad de ese objeto y su transmisión que son esenciales para su eficacia para autenticar; (b) la dependencia de credenciales costosas, estáticas, sembradas, incrustadas en el dispositivo móvil (tal como un certificado digital o un par de claves públicas/privadas) que deben administrarse para proporcionar los identificadores de usuario/dispositivo en lugar de realizar una afirmación en tiempo real, dinámica, construida a propósito e interactiva de esas identidades y contextos; (c) la dependencia de un conjunto separado de las credenciales anteriores (b) que se despliegan, siembran, administran y asocian para cada uno de los múltiples dispositivos móviles de un usuario; (d) el flujo unidireccional de la presentación de objetos para escanear para transmitir hacia el servicio autoritario en el extremo posterior, asume la integridad completa encriptada del proceso o el aislamiento de descomposición completo, y la inspección de las credenciales por la autoridad contra una base de datos almacenada de los datos literales; (e) el enfoque anterior (en (d)) elimina la función o el valor del dispositivo informático móvil en el proceso, ya que implica un mecanismo de captura y avance sin conocimiento del contexto o toma de decisiones mutua; (f) el último enfoque (en (d)) carga la autoridad para tomar la decisión de autenticación unilateral de forma aislada con las credenciales literales, abriendo el camino para la ingeniería inversa, repetición o predicción; (g) el enfoque de almacenar y reenviar niega la interacción del proceso y una conciencia más rica e inteligente de múltiples factores en profundidad dentro del tejido del contexto de la sesión; (h) la dependencia del servidor del sistema central (capa de presentación) para interactuar con el contenido codificado proporciona la oportunidad de inspección, pirateo, repetición, captura, modificación, compromiso; (i) la dependencia de la encriptación requiere capacidades de desencriptación y/o reencriptación iguales y opuestas del dispositivo informático móvil, extendiendo así la lógica del proceso de forma remota y la exposición al pirateo informático; (j) el riesgo de colapsar y mezclar los datos de identidad y autenticación a medida que el proceso envía identificadores a lo largo del mismo cable a través del código, el móvil y la mensajería al servidor autoritario proporciona numerosas oportunidades de ataques, integridad dudosa y falta de privacidad; (k) en servicio de la facilidad de uso excesiva al colapsar el escaneo de inicio de sesión (autoinformado) con la prueba de autenticación (credencial de teléfono almacenada estática), la limitación del proceso global con el único propósito de otorgar o denegar a un usuario el acceso a un recurso sin relación con la identidad adicional o los métodos de autenticación (*es decir*, ya no es una capa de defensa en profundidad) da como resultado que la técnica anterior sea un único punto de fallo; (l) la falta de triangulación, interrogatorio, medición y toma de decisiones interdependientes adecuadas con respecto a la fuente, la integridad y el estado del contexto de autenticación; (m) no tratar la autenticación como un contexto, simplemente un conjunto de credenciales para ser reenviadas; (n) no triangular las suposiciones físicas y digitales sobre la ubicación, la proximidad y el comportamiento, desde múltiples fuentes y perspectivas; y (o) la falta de participación activa y compromiso del usuario, dispositivo, contexto de sesión, ubicación, proximidad, comportamiento y contexto de triangulación en el proceso de autenticación.

Por lo tanto, en base a lo anterior, lo que se necesita es un método y sistema de autenticación que supere las deficiencias en los sistemas actualmente disponibles. La presente invención resuelve estas deficiencias y generalmente representa una innovación nueva y útil en el espacio de autenticación de factores contextuales a través de redes de autenticación.

Resumen de la invención

Para minimizar las limitaciones en la técnica anterior, y para minimizar otras limitaciones que serán evidentes tras la lectura y comprensión de la presente descripción, la presente invención describe un nuevo y útil sistema y método de autenticación de contexto de seguridad móvil.

Una modalidad de la presente invención es un método basado en ordenador para autenticar a un usuario a través de una red, las etapas que comprenden: proporcionar un sistema central, un servidor, una presentación y un dispositivo; en donde el dispositivo incluye una o más aplicaciones; en donde el servidor incluye un algoritmo de perfil; solicitar un acceso al sistema central por un usuario principal en la presentación a través de un canal de usuario; solicitar al servidor realizar una decisión de verificación de contexto por el sistema central sobre un canal del sistema central; crear dos o más objetos de plantilla por el algoritmo de perfil del servidor; en donde los dos o más objetos de plantilla son una primera plantilla y una segunda plantilla; enviar un objeto al sistema central a través del canal del sistema central por el servidor; presentar el objeto al dispositivo en la presentación y a través del canal de usuario por el sistema central; procesar la primera plantilla por el servidor; en donde la etapa de procesamiento de la primera plantilla se basa en uno o más factores contextuales; llenar la primera plantilla por el servidor; crear y almacenar una primera firma (en memoria) por el servidor; en donde la etapa de creación de la primera firma se basa en la etapa de procesamiento de la primera plantilla; consumir el objeto por el usuario principal en el dispositivo a través de la una o más aplicaciones; solicitar la segunda plantilla del servidor a través de un canal inteligente preferentemente codificado por la una o más aplicaciones; enviar la segunda plantilla a la una o más aplicaciones en el dispositivo a través del canal inteligente por el servidor; procesar la segunda plantilla por la una o más aplicaciones; llenar la segunda plantilla por la una o más aplicaciones; crear y almacenar una segunda firma (en memoria) por la una o más aplicaciones; en donde la etapa de creación de la segunda firma se basa en la segunda plantilla; y realizar la decisión de verificación de contexto cuando se compara la primera firma y la segunda firma a través del canal inteligente. El método basado en ordenador puede comprender además la etapa de proporcionar uno o más factores externos adicionales al dispositivo por parte del sistema central a través del canal fuera de banda. El método basado en ordenador puede comprender además la etapa de: eliminar el uno o más factores contextuales por parte del servidor. La etapa de procesamiento de la segunda plantilla puede realizarse en base a uno o más factores contextuales. La etapa de creación y almacenamiento de la primera firma puede basarse en la etapa de consumo del objeto. La etapa de creación y almacenamiento de la primera firma puede basarse en la etapa de procesamiento de la segunda plantilla. El método basado en ordenador puede comprender además las etapas de: introducir uno o más datos fuera de banda en la una o más aplicaciones; en donde el uno o más datos fuera de banda se transmiten a través del canal fuera de banda. La etapa de comparación de la primera firma y la segunda firma puede realizarse por el servidor. La etapa de comparación de la primera firma y la segunda firma puede realizarse por la una o más aplicaciones. El método basado en ordenador puede comprender además las etapas de: autenticar el dispositivo cuando la primera firma es esencialmente idéntica a la segunda firma.

Otra modalidad de la presente invención es un método basado en ordenador para autenticar a un usuario a través de una red, las etapas que comprenden: proporcionar un sistema central, un servidor, una presentación y un dispositivo; en donde el dispositivo incluye una o más aplicaciones; en donde el servidor incluye un algoritmo de perfil; solicitar un acceso al sistema central por un usuario principal en la presentación a través de un canal de usuario; solicitar al servidor realizar una decisión de verificación de contexto por el sistema central sobre un canal del sistema central; crear una primera plantilla y una segunda plantilla por el algoritmo de perfil del servidor; enviar un objeto al sistema central a través del canal del sistema central por el servidor; presentar el objeto al dispositivo en la presentación y a través del canal de usuario por el sistema central; procesar la primera plantilla por el servidor; en donde la etapa de procesamiento de la primera plantilla se basa en un primer conjunto de uno o más factores contextuales; llenar la primera plantilla por el servidor; crear y almacenar una primera firma (en memoria) por el servidor; en donde la etapa de creación de la primera firma se basa en la etapa de procesamiento de la primera plantilla; consumir el objeto por el usuario principal en el dispositivo a través de la una o más aplicaciones; solicitar la segunda plantilla del servidor a través de un canal inteligente preferentemente codificado por la una o más aplicaciones; enviar la segunda plantilla a la una o más aplicaciones en el dispositivo a través del canal inteligente por el servidor; procesar la segunda plantilla por la una o más aplicaciones; llenar la segunda plantilla por la una o más aplicaciones; crear y almacenar una segunda firma (en memoria) por la una o más aplicaciones; en donde la etapa de creación de la segunda firma se basa en la segunda plantilla; realizar la decisión de verificación de contexto cuando se compara la primera firma y la segunda firma a través del canal inteligente; y autenticar el dispositivo cuando la primera firma es esencialmente idéntica a la segunda firma. El método basado en ordenador puede comprender además las etapas de: proporcionar uno o más factores externos adicionales al dispositivo por parte del sistema central a través del canal fuera de banda. El método basado en ordenador puede comprender además las etapas de: eliminar el uno o más factores contextuales por el servidor. La etapa de procesamiento de la segunda plantilla puede realizarse en base a un segundo conjunto de uno o más factores contextuales. La etapa de creación y almacenamiento de la primera firma puede basarse en la etapa de consumo del objeto. La etapa de creación y almacenamiento de la primera firma puede basarse en la etapa de procesamiento de la segunda plantilla. El método basado en ordenador puede comprender además las etapas de: introducir uno o más datos

fuera de banda en la una o más aplicaciones; en donde el uno o más datos fuera de banda se transmiten a través del canal fuera de banda. La etapa de comparación de la primera firma y la segunda firma puede realizarse por el servidor. La etapa de comparación de la primera firma y la segunda firma puede realizarse por la una o más aplicaciones.

Otra modalidad de la presente invención es un método basado en ordenador para autenticar a un usuario a través de una red, las etapas que comprenden: proporcionar un sistema central, un servidor, una presentación y un dispositivo; en donde el dispositivo incluye una o más aplicaciones; en donde el servidor incluye un algoritmo de perfil; solicitar un acceso al sistema central por un usuario principal en la presentación a través de un canal de usuario; solicitar al servidor realizar una decisión de verificación de contexto por el sistema central sobre un canal del sistema central; crear una primera plantilla y una segunda plantilla por el algoritmo de perfil del servidor; enviar un objeto al sistema central a través del canal del sistema central por el servidor; presentar el objeto al dispositivo en la presentación y a través del canal de usuario por el sistema central; procesar la primera plantilla por el servidor; en donde la etapa de procesamiento de la primera plantilla se basa en uno o más factores contextuales; llenar la primera plantilla por el servidor; crear y almacenar una primera firma (en memoria) por el servidor; en donde la etapa de creación de la primera firma se basa en la etapa de procesamiento de la primera plantilla; en donde la etapa de creación y almacenamiento de la primera firma se basa en la etapa de consumo del objeto; consumir el objeto por el usuario principal en el dispositivo a través de la una o más aplicaciones; solicitar la segunda plantilla del servidor a través de un canal inteligente por la una o más aplicaciones; enviar la segunda plantilla a la una o más aplicaciones en el dispositivo a través del canal inteligente por el servidor; procesar la segunda plantilla por la una o más aplicaciones; en donde la etapa de procesamiento de la segunda plantilla se basa en uno o más factores contextuales; llenar la segunda plantilla por la una o más aplicaciones; crear y almacenar una segunda firma (en memoria) por la una o más aplicaciones; eliminar el uno o más factores contextuales por el servidor; en donde la etapa de creación de la segunda firma se basa en la segunda plantilla; realizar la decisión de verificación de contexto cuando se compara la primera firma y la segunda firma a través del canal inteligente por el servidor y la una o más aplicaciones; y autenticar el dispositivo cuando la primera firma es esencialmente idéntica a la segunda firma.

Otra modalidad de la invención se ilustra donde un usuario desea iniciar sesión en un sitio web o aplicación. Generalmente, el usuario desea acceder a un sistema central o sitio web a través de un canal de usuario desde su ordenador u otro tipo de dispositivo de unidad de procesamiento de datos electrónicos a través de un navegador e iniciar sesión mediante el uso de un nombre de usuario/contraseña tradicional, sus combinaciones, y/o etapa de identificación de inicio de sesión único. El sitio web entonces contacta preferentemente al servidor a través de un canal del sistema central tal como un canal de comunicación privado con una solicitud para autenticarse. En respuesta, el servidor preferentemente devuelve un objeto, tal como un código QR, un código de texto o un hipervínculo para presentar al usuario. El servidor crea preferentemente además dos o más plantillas en su memoria (una primera plantilla para su propio procesamiento y una segunda plantilla para el consumo del dispositivo o unidad de procesamiento de datos electrónicos del usuario). Adicionalmente, el sitio web generalmente presenta un objeto o un objeto de enlace de vuelta al usuario a través de una presentación, tal como un canal del navegador. Cuando usa una aplicación en su dispositivo, el usuario selecciona el objeto escaneando, detectando, ingresando, o respondiendo al objeto o al objeto de enlace. Como resultado, la aplicación preferentemente sigue al objeto para recuperar la segunda plantilla directamente, de forma privada e independientemente del servidor a través de un canal inteligente, que es preferentemente un tercer canal discreto, encriptado y nuevo, separado del canal de usuario y el canal del sistema central. El servidor entonces llena preferentemente la primera plantilla con los factores contextuales tales como los elementos del contexto de la sesión (p. ej., el servidor del sistema central, la ubicación de la presentación del objeto de enlace/código, el usuario, el dispositivo, la ubicación, cualquier credencial suministrada o algoritmos almacenados en la nube sobre el comportamiento del usuario, atributos o historial). Mediante el uso de tales factores contextuales desde la perspectiva del servidor, el servidor preferentemente llena de manera algorítmica la primera plantilla para construir una primera firma - *es decir*, una firma de contexto de un uso en la memoria. De manera simultánea o aproximadamente al mismo tiempo, la aplicación en el dispositivo del usuario preferentemente llena de manera aleatoria los factores contextuales similares desde la perspectiva del dispositivo mediante el uso de elementos del sitio web, el servidor, el dispositivo en sí, el usuario y la sesión. Esta etapa preferentemente resulta con el dispositivo del usuario que llena independientemente la segunda plantilla para construir algorítmicamente una segunda firma. La segunda firma puede correlacionarse o entrar en conflicto potencialmente con la primera firma del servidor. Además, el usuario puede "realizar" ciertas acciones de comportamiento (*p. ej*., mirar hacia el norte, orientar el móvil en modo vertical o ejecutar un gesto, o "existir" dentro de ciertos atributos de ubicación o proximidad tales como la proximidad a la pantalla de visualización del servidor u otro dispositivo o punto de ubicación fijo), que se interrogan preferentemente además en tiempo real y fortalecen aún más la segunda firma del usuario. Cualquier dato del rendimiento esperado, ubicación, proximidad, u otros factores contextuales de un usuario o dispositivo anterior, puede crear una modificación complementaria del algoritmo en el servidor. Independientemente del número, composición y profundidad de las entradas (*es decir*, una firma de múltiples masas), las plantillas y firmas son preferentemente únicas y distintas entre sí y cualquier otro objeto anterior o futuro. Preferentemente, las primera y segunda firmas no se reutilizan ni reproducen, sino que se modifican mediante nuevas entradas, atributos y factores contextuales. Al finalizar la creación de las primera y segunda firmas, el servidor y el dispositivo preferentemente comparan sus firmas respectivas a través del canal inteligente, evitando el canal de usuario (*p. ej*., el navegador) y el canal del sistema central. Si la primera firma y la segunda firma coinciden, el contexto completo preferentemente se autentica mutuamente. Por otro lado, si la primera firma y la segunda firma no coinciden, el contexto mutuo preferentemente no se autentica. Preferentemente, no se capturan ni transmiten información o pares de clave-valor, sino que se aplican algorítmicamente una vez en el extremo del servidor y el extremo del usuario. El

servidor preferentemente informa al usuario, dispositivo y al sistema central el estado de autenticación, y las partes pueden proceder apropiadamente en base a los resultados de la autenticación. Todos los componentes de la sesión se destruyen preferentemente en la memoria, y no se almacena, escribe, lee, recupera o siembra ninguna información preferentemente hacia o desde el dispositivo durante ninguna parte del proceso de autenticación.

La presente invención proporciona un nuevo método y sistema para proporcionar seguridad de red, ya que la autenticación requiere la separación, triangulación, interrogación contextual y toma de decisiones equitativa y mutua en un espacio tradicionalmente restringido por la ofuscación, la confidencialidad compartida y la administración autoritaria y la afirmación de credenciales y la verificación. Al enfrentar un nuevo ámbito de la World Wide Web, la informática en la nube, la informática móvil, y la interacción social, la presente invención ha abordado la evolución de mantener una custodia de las credenciales de autenticación, (cuyas partes (o pares) se consideran que requieren, evalúan o establecen confianza) a la autenticación basada en contexto donde el contexto de autenticación proporciona mayor seguridad y autenticación. La presente invención va más allá del acceso remoto tradicional o el acceso cliente-servidor.

La presente invención preferentemente descarta los métodos convencionales de autenticación de secreto compartido o captura y reenvío para crear un nuevo mecanismo más inteligente y a prueba del futuro para la seguridad de la red que abarca las realidades de las conexiones, las credenciales, las autoridades, los comportamientos, las redes, la movilidad, los pares y los contextos de realidad aumentada en la era digital social y móvil.

Es un objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que preferentemente logre una verificación y autenticación fuerte, elegante, privada, definitiva y en tiempo real en el contexto de un usuario, dispositivo, sitio/sesión, servidor, ubicación y atributos de comportamiento dentro de una sesión definida y a través de una red desde un dispositivo informático electrónico móvil. La invención preferentemente logra este objetivo y presenta una verdadera innovación de autenticación empleando los siguientes tres nuevos componentes: (1) la verificación de credenciales de contexto mutua de múltiples factores sintetizada, en tiempo real, no identificable desde múltiples perspectivas más allá de un canal de sesión principal; (2) la línea móvil de triangulación de visión/sonido/detección de la ubicación y proximidad digital y física; y (3) la mejora de la seguridad de autenticación aditiva impulsada por el usuario, con verificación y control a través de la personalización y/o los factores de "ludificación" tales como la ubicación, la proximidad, el comportamiento o la personalización a través de la compra o habilitación en la aplicación, la configuración y el rendimiento.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice firmas de autenticación sintetizadas, de múltiples masas y construidas a propósito de múltiples factores de contexto en lugar de inspeccionarlas individualmente y transmitirlas como pares clave-valor.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice una verificación y autenticación de tejido contextual basada en plantilla y algorítmica.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice un proceso y decisión de coincidencia no unilateralmente autoritario a través de todos los miembros, canales igualmente, en lugar de una única fuente patriarcal de autoridad o secreto.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que no dependa de cookies, certificados, la información sembrada o persistente, las claves públicas/privadas, los secretos compartidos, las contraseñas, el conocimiento del usuario o los factores biométricos en el sistema central, el servidor de la invención o las capas de usuario/dispositivo.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice flujos de canales de comunicación de datos bidireccionales, separados y triangulados entre las partes, eliminando así un único punto de fallo, intercepción o ruta.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice la inspección e interrogación de factores contextuales en múltiples perspectivas.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que no dependa de los secretos codificados, encriptados o incrustados, identificando la información dentro del enlace u objeto de activación, código, imagen, sonido/señal o vibración (*p. ej.,* el código QR).

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice el procesamiento algorítmico automático en tiempo real en un servidor y dispositivo móvil; sin almacenar, sembrar, administrar y transmitir los datos discretos o credenciales.

Otro objetivo de la presente invención es proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice la inscripción dinámica y la autenticación a través de todos los dispositivos móviles de los usuarios en vez de la siembra, coincidencia y asociación de credenciales dispositivo por dispositivo.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice una autenticación privada no identificable de usuarios, dispositivos, sitios, sesiones, factores.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice una verificación de contexto física de la línea de visión/sonido/sensación de las suposiciones digitales.

Es otro objetivo de la presente invención proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice tecnología, protocolo y/o implementación agnóstica de plataformas a través de múltiples dispositivos.

Otro objetivo de la presente invención es proporcionar un sistema y método de autenticación de contexto de seguridad móvil que utilice factores de personalización de autenticación controlados por el usuario tales como: el comportamiento, el contexto, la ubicación, a través de opciones y configuración en la aplicación.

Es un objetivo de la presente invención proporcionar un nuevo y novedoso sistema y método que ofrezca una solución superior en el campo, la ciencia y el área de la autenticación electrónica.

Es un objetivo de la presente invención superar las limitaciones de la técnica anterior.

Estos, así como también otros componentes, etapas, características, objetivos, beneficios y ventajas, quedarán claros a partir de una revisión de la siguiente descripción detallada de las modalidades ilustrativas, los dibujos adjuntos y las reivindicaciones.

Breve descripción de las figuras

Los dibujos son de modalidades ilustrativas. Los dibujos no ilustran todas las modalidades. Pueden usarse otras modalidades además o en su lugar. Los detalles que pueden ser evidentes o innecesarios pueden omitirse para ahorrar espacio o para una ilustración más efectiva. Algunas modalidades pueden llevarse a la práctica con componentes o etapas adicionales y/o sin todos los componentes o etapas que se ilustran. Cuando aparece el mismo número en diferentes dibujos, se refiere a los mismos o similares componentes o etapas.

La Figura 1 es una tabla de léxico que muestra una colección de caracteres alfanuméricos que ayudan a explicar, junto con la presente descripción, uno o más símbolos en las siguientes figuras.

La Figura 2 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra las funciones y etapas entre un sistema central, servidor, usuario principal, dispositivo, aplicación y presentación desde la presentación al dispositivo.

La Figura 3 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra las funciones y etapas entre un sistema central, un usuario, un dispositivo, y la aplicación a aplicación desde dentro del dispositivo.

La Figura 4 es un diagrama de flujo de bloques funcional de una modalidad del proceso de ludificación del sistema y método de autenticación de contexto de seguridad móvil y muestra las etapas iniciales del proceso de ludificación-*es decir*, seleccionar y configurar los factores contextuales tales como los factores de ubicación, los factores de comportamiento y los factores de personalización.

La Figura 5 es un diagrama de flujo de bloques funcional de una modalidad del proceso de ludificación del sistema y método de autenticación de contexto de seguridad móvil y muestra las últimas etapas del proceso de ludificación-*es decir*, procesar la primera plantilla por el servidor y la segunda plantilla por la aplicación del dispositivo.

La Figura 6 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra la triangulación entre el sistema central, la presentación, el dispositivo y el servidor.

Descripción detallada de la invención

En la siguiente descripción detallada de varias modalidades de la invención, se exponen numerosos detalles específicos para proporcionar una comprensión completa de varios aspectos de una o más modalidades de la invención. Sin embargo, una o más modalidades de la invención pueden llevarse a la práctica sin algunos o todos estos detalles específicos. En otros casos los métodos, procedimientos y componentes bien conocidos no se han descrito en detalle para no oscurecer innecesariamente los aspectos de las modalidades de la invención.

Aunque se describen múltiples modalidades, aún otras modalidades de la presente invención serán evidentes para los expertos en la técnica a partir de la siguiente descripción detallada, que muestra y describe modalidades ilustrativas de la invención. Como se comprenderá, la invención es capaz de modificaciones en varios aspectos obvios, todo ello sin apartarse del alcance de la presente invención. Por consiguiente, los gráficos, las figuras y las descripciones detalladas

de los mismos, deben considerarse de naturaleza ilustrativa y no restrictiva. Además, la referencia o la no referencia a una modalidad particular de la invención no deberá interpretarse como que limita el alcance de la invención.

En la siguiente descripción, se usa cierta terminología para describir ciertas características de una o más modalidades de la invención. Por ejemplo, los términos "dispositivo", "ordenador", "unidad de procesamiento de datos electrónicos", "servidor de invención" o "servidor" se refieren a cualquier dispositivo que procesa información con un chip de circuito integrado, que incluye, sin limitación, ordenadores personales, ordenadores de unidad central, estaciones de trabajo, servidores, ordenadores de escritorio, ordenadores portátiles, ordenadores integrados, dispositivos inalámbricos que incluyen teléfonos celulares, asistentes digitales personales, tabletas, ordenadores de tabletas, teléfonos inteligentes, reproductores de juegos portátiles y ordenadores de mano. El término "internet" se refiere a cualquier colección de redes que utiliza protocolos estándares, ya sea Ethernet, Token ring, Wifi, Modo de transferencia asíncrona (ATM), Interfaz para datos distribuidos por fibra (FDDI), Código de división de múltiples accesos (CDMA), Sistemas globales para comunicaciones móviles (GSM), Evolución a largo plazo (LTE) o cualquiera de sus combinaciones. El término "sitio web" se refiere a cualquier documento escrito en un lenguaje de marcado que incluye, pero no se limita a, lenguaje de marcado de hipertexto (HTML) o lenguaje de modelado de realidad virtual (VRML), HTML dinámico, lenguaje de marcado extendido (XML), lenguaje de marcado inalámbrico (WML) o cualquier otro lenguaje informático relacionado a este, así como también cualquier colección de dichos documentos accesibles a través de una dirección de protocolo de Internet específica o en un sitio específico de la World Wide Web, o cualquier documento que pueda obtenerse a través de cualquier Localizador uniforme de recursos (URL). Además, los términos "página web", "página", "sitio web" o "sitio" se refieren a cualquiera de los diversos documentos y recursos en la World Wide Web, en formato HTML/XHTML con enlaces de hipertexto para permitir la navegación desde una página o sección a otra, o similar a dichos recursos usados en la Internet.

El término "factor" se refiere a cualquier factor, que incluye factores de múltiples masas, durante la sesión de autenticación principal, que incluye sin limitación, factores de contexto de autenticación personalizados o factores personales (p. ej., factores de ubicación, factores de comportamiento, factores de personalización, factores de proximidad); elementos o factores del contexto de sesión en la perspectiva del servidor (p. ej., servidor del sistema central, ubicación de la presentación del objeto de enlace/código, usuario, dispositivo, ubicación, cualquier credencial suministrada o algoritmo almacenado en la nube sobre el comportamiento, los atributos o el historial del usuario); elementos del contexto de sesión en la perspectiva del dispositivo (*p. ej.*, elementos del sitio web, servidor, dispositivo en sí, usuario y sesión); acciones de comportamiento del usuario (*p. ej.,* mirar hacia el norte, orientar el móvil en modo vertical o ejecutar un gesto, o "existir" dentro de ciertos atributos de ubicación o proximidad tales como la proximidad a la pantalla de visualización del servidor u otro dispositivo o punto de ubicación fijo); y factores externos tales como uno o más números de identificación personal fuera de banda (PIN), frase de contraseña, datos secretos compartidos, contraseña de un solo uso o contraseña reutilizada, entregados por correo electrónico, servicio de mensajes cortos (SMS), servicio multimedia (MMS), voz, ficha física u otra transmisión mediada por humanos o por ordenador fuera del canal de usuario, el canal del sistema central y el canal inteligente.

La presente invención es preferentemente un método y sistema de seguridad de autenticación de contexto de factores múltiples que usa uno o más dispositivos informáticos electrónicos a través de una red y uno o más factores contextuales dentro de una sesión definida. Una modalidad de la invención se produce cuando un usuario desea iniciar sesión en un sitio web o aplicación. El usuario puede acceder a un sistema central o sitio web a través de un canal de usuario desde su ordenador u otro tipo de dispositivo de unidad de procesamiento de datos electrónicos a través de un navegador y preferentemente inicia sesión mediante el uso de un nombre de usuario/contraseña tradicional, sus combinaciones, y/o etapa de identificación de inicio de sesión único. El sitio web entonces preferentemente contacta al servidor a través de un canal del sistema central como un canal de comunicación privado con una solicitud para autenticarse. En respuesta, el servidor preferentemente devuelve un objeto, tal como un código QR, un código de texto o un hipervínculo para presentar al usuario. El servidor crea preferentemente además dos o más plantillas en su memoria (una primera plantilla para su propio procesamiento y una segunda plantilla para el consumo del dispositivo o unidad de procesamiento de datos electrónicos del usuario). Adicionalmente, el sitio web generalmente presenta un objeto o un objeto de enlace de vuelta al usuario a través de una presentación, tal como un canal del navegador. Cuando usa una aplicación en su dispositivo, el usuario selecciona o consume el objeto escaneando, detectando, ingresando, o respondiendo al objeto. Como resultado, la aplicación preferentemente sigue al objeto para recuperar la segunda plantilla directamente, de forma privada e independientemente del servidor a través de un canal inteligente, que es preferentemente un tercer canal discreto nuevo, separado del canal de usuario y el canal del sistema central. El servidor entonces llena preferentemente la primera plantilla con los factores contextuales tales como los elementos del contexto de la sesión (p. ej., el servidor del sistema central, la ubicación de la presentación del objeto de enlace/código, el usuario, el dispositivo, la ubicación, cualquier credencial suministrada o algoritmos almacenados en la nube sobre el comportamiento del usuario, atributos o historial). Mediante el uso de tales factores contextuales desde la perspectiva del servidor, el servidor preferentemente, llena de manera algorítmica la primera plantilla para construir una primera firma-*es decir*, una firma de contexto de un uso en la memoria. De manera simultánea o aproximadamente cerca del mismo tiempo, la aplicación en el dispositivo del usuario preferentemente llena de manera aleatoria los factores contextuales similares desde la perspectiva del dispositivo mediante el uso de elementos del sitio web, el servidor, el dispositivo en sí, el usuario y la sesión. Esta etapa preferentemente resulta con el dispositivo del usuario que llena independientemente la segunda plantilla para construir algorítmicamente una segunda firma. La segunda firma puede correlacionarse o entrar en conflicto potencialmente con la primera firma del servidor. Además, el usuario puede

"realizar" ciertas acciones de comportamiento (*p. ej.*, mirar hacia el norte, orientar el móvil en modo vertical o ejecutar un gesto, o "existir" dentro de ciertos atributos de ubicación o proximidad tales como la proximidad a la pantalla de visualización del servidor u otro dispositivo o punto de ubicación fijo), que se interrogan preferentemente además en tiempo real y fortalecen aún más la segunda firma del usuario. Cualquier dato del rendimiento esperado, ubicación, proximidad, u otros factores contextuales de un usuario o dispositivo anterior, puede crear una modificación complementaria del algoritmo en el servidor. Independientemente del número, composición y profundidad de las entradas (*es decir*, una firma de múltiples masas), las plantillas y firmas son preferentemente únicas y distintas entre sí y cualquier otro objeto anterior o futuro. Preferentemente, las primera y segunda firmas no se reutilizan ni reproducen, sino que se modifican mediante nuevas entradas, atributos y factores contextuales. Al finalizar la creación de las primera y segunda firmas, el servidor y el dispositivo preferentemente comparan sus firmas respectivas a través del canal inteligente, evitando el canal de usuario (*p. ej.*, el navegador) y el canal del sistema central. Si la primera firma y la segunda firma coinciden, el contexto completo preferentemente se autentica mutuamente. Por otro lado, si la primera firma y la segunda firma no coinciden, el contexto mutuo preferentemente no se autentica. Generalmente, no se capturan ni transmiten información o pares de clave-valor, sino que se aplican algorítmicamente una vez en el extremo del servidor y el extremo del usuario. El servidor preferentemente informa al usuario, dispositivo y al sistema central el estado de autenticación y, como resultado, las partes pueden proceder apropiadamente, en dependencia de los resultados de la autenticación. Todos los componentes de la sesión se destruyen preferentemente en la memoria, y no se almacena, escribe, lee, recupera o siembra ninguna información preferentemente hacia o desde el dispositivo durante ninguna parte del proceso de autenticación.

La Figura 1 es una tabla de léxico que muestra una colección de caracteres alfanuméricos que ayudan a explicar, junto con la presente descripción, uno o más símbolos en las siguientes figuras. Por ejemplo, el símbolo "U1" preferentemente se refiere al usuario principal. Adicionalmente, el símbolo "H1" generalmente se refiere al sistema central o sistema central principal. Aunque se describen múltiples símbolos para representar y explicar diversas modalidades de la presente invención, la invención es capaz de modificaciones en diversos aspectos obvios, ya que los símbolos deben considerarse de naturaleza ilustrativa y no restrictivos.

Parte 1- autenticación

La Figura 2 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra las funciones y etapas entre un sistema central, un servidor, un usuario principal, un dispositivo, una aplicación y una presentación desde la presentación al dispositivo. Como se muestra en la Figura 2, una modalidad del sistema y método de autenticación de contexto de seguridad móvil 201 incluye preferentemente: un usuario principal 205; un dispositivo 210; una presentación 213; un sistema central 215; un servidor 218; una aplicación 220; un canal de usuario 222; un canal del sistema central 224; un canal inteligente 226; un canal fuera de banda 228; un algoritmo de perfil 230; una primera plantilla 232; una segunda plantilla 235; un objeto 238; una primera firma 240; y una segunda firma 243. Además, las etapas 1, 2, 3, 4, 4a, 5, 6, 7, 7a, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 de una modalidad del sistema y método de autenticación de contexto de seguridad móvil 201 se referencian preferentemente mediante números en las figuras.

El usuario principal 205 generalmente es cualquier individuo que desee autenticar una sesión de comunicación con el sistema central 215 y el servidor 218 mediante el uso de una autenticación en tiempo real, mutua, triangular y de múltiples factores en un dispositivo 210, mediante el uso de la aplicación 220 desde la pantalla o presentación 213 al dispositivo 210. El dispositivo 210 típicamente es una unidad de procesamiento de datos electrónicos que realiza diversas funciones a través de su aplicación 220, tales como el escaneo y detección, y es preferentemente capaz de conectarse en red. La presentación 213 en la presente modalidad es preferentemente una pantalla o emisor unidireccional para el escaneo, clic, entrada, detección, consumo o procesamiento y decodificación por el usuario principal 205 en el dispositivo 210 a través de la aplicación 220. Preferentemente, el escaneo para transmitir hacia el servicio autoritario en el extremo posterior incluye una integridad encriptada completa del proceso o un aislamiento completo de la descomposición, y la inspección de las credenciales por la autoridad contra una base de datos almacenada de datos literales. El sistema central 215 es típicamente cualquier ordenador independiente, dispositivo informático móvil, unidad de procesamiento de datos electrónicos, servidor, aplicación o sitio web que se conecta a una red, que puede proporcionar recursos de información, servicios y aplicaciones a usuarios u otros nodos en la red. El servidor 218 es preferentemente cualquier ordenador, programa informático o unidad de procesamiento de datos electrónicos que ayude a gestionar el acceso a un recurso o servicio centralizado en una red. La aplicación 220 es preferentemente una o más piezas de software que hacen que el dispositivo 210, el ordenador o la unidad de procesamiento de datos electrónicos realice cualquier tarea útil más allá del funcionamiento del ordenador en sí.

El canal de usuario 222, el canal del sistema central 224, el canal inteligente 226, y el canal fuera de banda 228 son preferentemente canales separados de comunicaciones dentro de una red, independientes entre sí. Específicamente, el canal de usuario es preferentemente una banda de frecuencia específica para la transmisión y recepción de señales electromagnéticas entre la presentación 213 y el sistema central 215. El canal del sistema central 224 es preferentemente una banda de frecuencia específica para la transmisión y recepción de señales electromagnéticas entre el sistema central 215 y el servidor 218. El canal inteligente 226 es preferentemente una banda de frecuencia específica para la transmisión y recepción de señales electromagnéticas entre el servidor 218 y el dispositivo 210. El canal fuera de banda 228 es preferentemente una o más bandas de frecuencias específicas fuera del canal inteligente

226 para la transmisión y recepción de señales electromagnéticas entre el servidor 218 y el dispositivo 210 con fines de autenticación.

El algoritmo de perfil 230 es preferentemente el elemento persistente, función u objeto del servidor 218 para el procesamiento y preferentemente representa un contexto único de un usuario, dispositivo, sitio, sesión, comportamiento, ubicación, proximidad y factores de personalización. Generalmente, cada contexto tiene un algoritmo único almacenado en el servidor 218 o nube del servidor ya sea generado en el primer registro o referido a la autenticación posterior para la generación de plantillas y el procesamiento resultante.

La primera plantilla 232 y la segunda plantilla 235 son preferentemente cualquier archivo, tipo de archivo o combinación de elementos de codificación que son desechables, creados a propósito, sustitutos, de contexto específico y dinámicos en masa (tamaño, secuencia, formato, estructura, profundidad y cantidad de registros) cuya composición y algoritmo de llenado se define por el contexto y el procesamiento de miembros.

El objeto 238 o el objeto de enlace es preferentemente cualquier elemento de enlace que se coloca generalmente dentro de un archivo o escritura para el consumo por el usuario principal en la aplicación 220 del dispositivo 210 mediante el escaneo, detección, clic o introducción manual del objeto en la aplicación 220; en forma de programa con la aplicación 220; o desde la presentación 213 al dispositivo 210 a través del canal del sistema central 224.

La primera firma 240 y la segunda firma 243 son preferentemente cualquier elemento en el archivo o el archivo en sí usado para autenticar cada servidor, estación cliente, dispositivo informático móvil o unidad de procesamiento de datos electrónicos durante la sesión de autenticación.

Con referencia a la Figura 2, la primera etapa 1 del sistema y método de autenticación de contexto de seguridad móvil 200 ocurre generalmente cuando el usuario principal 205 solicita acceso a un sistema central de recursos 215 tal como un sistema central 215. Específicamente, el usuario principal 205 preferentemente solicita acceso a un recurso y puede realizar una acción a través de una red, que requiere privilegio o autenticación en el servidor 218 o el servidor del sistema central en la presentación 213 a través del canal de usuario 222 desde el dispositivo 210 del usuario principal 205 en una sesión o contexto fijo. La sesión o contexto fijo puede ocurrir dentro de, entre, o en medio de un navegador, una aplicación, un programa, una red, un servidor, o una unidad fija de procesamiento de datos electrónicos o una unidad móvil de procesamiento de datos electrónicos.

La Figura 2 muestra además la segunda etapa 2, que preferentemente se realiza cuando el sistema central 215 solicita al servidor 218 a través del canal del sistema central 224 para realizar una decisión de verificación de contexto o autenticación con respecto al contexto del usuario principal 205/dispositivo 210/sistema central 215 dentro de una sesión principal o definida a través del canal inteligente 226. Esto requiere típicamente basarse en un único evento o en una capa de decisión sobre la identidad existente u otro proceso de autenticación. La decisión de verificación de contexto 245 es generalmente una verificación de contexto de múltiples masas, triangulada en el canal, en tiempo real, multiautoritaria basada en los factores contextuales a través del sistema central 215, el dispositivo 210/usuario principal 205, o múltiples sistemas centrales y múltiples dispositivos/usuarios, a través de múltiples canales y perspectivas del servidor 218 y el dispositivo 210. La decisión de verificación de contexto 245 se diseña preferentemente para autenticar y verificar la autenticidad del contexto holístico, en lugar de la identidad de miembros o factores aislados del sistema central 215, el usuario principal 205, el dispositivo 210 o el servidor 218 en el marco de autenticación convencional tradicional.

La Figura 2 muestra además la segunda etapa opcional 2a, que puede realizarse cuando el sistema central 215 proporciona factores externos adicionales (con relación al usuario principal 205 o el dispositivo 210) al dispositivo. Los factores externos adicionales pueden entregarse a través de un canal fuera de banda 228 al usuario principal 205 o el dispositivo 210, para el uso posterior. Los factores externos adicionales pueden incluir, pero no se limitan a: uno o más de números de identificación personal fuera de banda (PIN), frase de contraseña, datos secretos compartidos, contraseña de un solo uso o contraseña reutilizada, enviados por correo electrónico, servicio de mensajes cortos (SMS), servicio multimedia (MMS), voz, ficha física u otra transmisión mediada por humanos o por ordenador fuera del canal de usuario 222, el canal del sistema central 224 y el canal inteligente 226.

En respuesta, como se muestra en la Figura 2 en la tercera etapa 3, el servidor 218 construye preferentemente (a solicitud del sistema central 215 a través del canal del sistema central 224) dos o más objetos de plantilla basados en la síntesis de los factores de la sesión principal, el algoritmo de perfil generado 230, y/o valores aleatorios. Los objetos de plantilla (*p. ej.*, la primera plantilla 232 y la segunda plantilla 235) son preferentemente elementos de datos diferentes, creados a propósito, desechables y universalmente únicos que se almacenan en la memoria del servidor 218. Los dos o más objetos de plantilla se construyen y procesan preferentemente mediante el algoritmo de perfil 230, que típicamente es un objeto generado (autenticación de usuario por primera vez) o un objeto almacenado en la nube. Como se discutió anteriormente, los dos o más objetos de plantilla son preferentemente una primera plantilla 232 y una segunda plantilla 235; en donde la primera plantilla 232 preferentemente se genera completamente a partir del algoritmo de perfil 230 para el autoconsumo y procesamiento del servidor 218, mientras la segunda plantilla 235 sólo se genera parcialmente para la transmisión, el consumo, el llenado y el procesamiento por el usuario principal 205 o el dispositivo 210. Preferentemente, ni la primera plantilla 232 ni la segunda plantilla 235 contienen ni revelan ninguna relación con el

algoritmo de perfil 230, el número de identificación del usuario/dispositivo, el sistema central 215 y los detalles de la sesión. La primera plantilla 232 y la segunda plantilla 235 son preferentemente, y meramente contenedores parciales universalmente únicos para llenarse y procesarse de manera independiente y algorítmica en tiempo real durante el proceso de autenticación de la invención.

Con respecto a la cuarta etapa 4, el servidor 232 preferentemente devuelve al sistema central 215 un objeto 238 o un objeto de enlace a través del canal del sistema central 224 (en lugar de los valores de objeto reales o incluso sustitutos). El objeto 238 preferentemente proporciona una referencia para enlazar el usuario principal 205 con la segunda plantilla 235 del objeto destino, como se muestra en la Figura 2.

Adicionalmente, en la cuarta etapa 4a mostrada en la Figura 2, el sistema central 215 preferentemente presenta, muestra o emite un objeto 238 al usuario principal 205/dispositivo 210 en la presentación 213 a través del canal de usuario 222 para escanear, hacer clic, ingresar, detectar, consumir o procesar y descodificar por el usuario principal 205 en el dispositivo 210 a través de la aplicación 220. Debido a las oportunidades o restricciones ambientales de la sesión, la ruta o enlace a la segunda plantilla 235 puede llevarse a la práctica por el objeto 238 para el consumo por el dispositivo 210/usuario principal 205, en cualquiera de, pero sin limitarse a, los siguientes formatos: un código visual o audible (código QR, imagen, etiqueta, cadena, hipervínculo, sonido) escaneado o detectado por un dispositivo móvil capaz, un código manual (correo electrónico, tweet, mensaje directo (DM), servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS), hipervínculo, llamada de procedimiento remoto (RPC) tecleada por un usuario, código programático (mensaje en memoria, interfaz de programación de aplicaciones (API), llamada de función o método en aplicación a aplicación (como se muestra en la Figura 2) u otra transmisión (comunicación de campo cercano (NFC), dispositivo/vibración ambiental, golpe o movimiento del dispositivo, mensaje contextual, gesto, comportamiento, desafío/respuesta, actividad de usuario "ludificada" en la presentación 213 o el dispositivo 210 de habilidad o probabilidad).

En memoria, el servidor 218 preferentemente interroga, mide y llena dinámicamente su primera plantilla 232 generada por algoritmo de perfil con cualquier observación de factor contextual de la presente sesión de una o más informaciones o atributos con respecto a: la sesión, el sistema central 215, la presentación 213, el dispositivo 210, el usuario principal 205, la ubicación del sistema central, la ubicación de la presentación, la ubicación del dispositivo, la ubicación del usuario, el canal del usuario, cualquier factor externo transmitido, y ya sea almacenado o proporcionado en su sistema central 215, el conocimiento de los factores del dispositivo y los factores de personalización (*p. ej.*, comportamiento, ubicación, proximidad, personalización) para el usuario principal 205. En particular, el servidor 218 preferentemente mide, triangula y calcula la ubicación/proximidad física y digital (ubicación del usuario, ubicación del dispositivo, ubicación de la presentación, ubicación del sistema central) de la presentación 213/objeto 238 y el dispositivo 210, desde su perspectiva, a través de la medición del objeto 238/presentación 213 y el dispositivo 210 (como se muestra en la Figura 6). El servidor 218 luego preferentemente calcula y almacena en memoria una primera firma 240 dinámica y de algoritmo de firma creado a propósito, basada en la primera plantilla 232/sesión principal. El servidor 218 entonces preferentemente dispone todos los datos relacionados con el factor de múltiples masas (como se muestra en la Figura 2, quinta etapa 5).

El objeto 238 preferentemente se consume por el usuario principal 205 en el dispositivo 210 a través del escaneo, la detección, el clic o ingreso manual del objeto 238 a la aplicación 220; en forma de programa con la aplicación (transferencia de aplicación a aplicación, dentro del dispositivo); o desde la presentación 213 al dispositivo 210 (presentación al dispositivo) a través del canal del sistema central 224, como se muestra en la Figura 2, sexta etapa 6.

La aplicación 220 en el dispositivo 210 sigue preferentemente y de forma dinámica la ruta del objeto 238 a través del canal inteligente triangulado 226 de vuelta al servidor 218 para solicitar, recibir y consumir la segunda plantilla real nueva 235 de vuelta a través del canal inteligente 226. El consumo de la segunda plantilla 235 preferentemente no se restringe o limita al método mencionado anteriormente usado para transmitir y/o consumir el objeto 238 en sí. Pueden usarse además canales triangulados alternativos sin apartarse del alcance de la invención, como se muestra en la Figura 2, séptima etapa 7. El método de iniciación del proceso de autenticación de la presente invención es de manera típica drásticamente diferente del enfoque tradicional de captura, decodificación y reenvío de la mayoría de las técnicas basadas en código QR encontradas en los métodos convencionales, y representa un salto adelante en fortaleza, privacidad e integridad ya que el código/valor del objeto 238 de la presentación transmitida y la aplicación consumida en el dispositivo 210 es desechable y no privado o de identificación. Además, el punto de inicio generalmente representa la responsabilidad final del sistema central 215 y la presentación 213, a diferencia de los métodos convencionales, que deben incluir la información del sistema central o sesión dentro del código para el consumo y asociación con móviles estáticos o credenciales de usuario, y una transmisión pareada eventual de vuelta a un servidor de autenticación. En la presente invención, la ofuscación u ocultamiento de los datos codificados generalmente no es fundamental para su seguridad o funcionalidad, sino simplemente una ruta para una conexión de sesión más privada y controlada para el consumo del objeto de sesión de autenticación, y por lo tanto, un enfoque más robusto, seguro y novedoso.

A continuación, la aplicación 220 en el dispositivo 210 preferentemente consume la segunda plantilla 235 y se interroga a sí misma y al contexto en tiempo real, desde la perspectiva del dispositivo 210/usuario principal 205, como se muestra en la Figura 2, octava etapa 8. La aplicación 220 entonces llena preferentemente de manera algorítmica la segunda plantilla 235 con uno o más factores contextuales (factores del dispositivo, factores personales) con respecto a

cualquiera o todos de los siguientes: el sistema central 215, la ubicación del sistema central, la presentación 213, la ubicación de la presentación, el dispositivo 210, la ubicación del dispositivo, el usuario principal 205, la ubicación del usuario principal, el comportamiento del dispositivo, el comportamiento del usuario principal, el canal del dispositivo, el canal del usuario principal, el factor de fuera de banda, los factores del dispositivo, el factor de comportamiento, el factor de ubicación y el factor de personalización. La aplicación 220 a través del dispositivo 210 puede usar además sistema de posicionamiento global nativo (GPS), acelerómetro, protocolo de Internet (IP) para geolocalización, servicios, capacidades de software o hardware o tecnología personalizada para recolectar los factores contextuales y triangular su contexto de línea de visión/sentido con el objeto 238/presentación 213 y el servidor 218 con sus observaciones digitales de ubicación y proximidad, como se muestra en la Figura 6. Cada dispositivo informático móvil preferentemente será único para sí mismo con respecto a tales capacidades y, por lo tanto, sólo necesita coincidir consigo mismo y no con otros dispositivos con diferentes capacidades o acceso a los factores. La presente invención supera además los métodos de seguridad convencionales midiendo dinámicamente no sólo la ubicación absoluta (Geo, IP) de los miembros de la sesión (el sistema central 215, el dispositivo 210, el servidor 218) sino además la proximidad de los miembros activos (la presentación 213, la aplicación 220 en el dispositivo 210) por la naturaleza de verificar tanto la proximidad de la línea de visión/sonido como la proximidad digital desde múltiples perspectivas. Este método es generalmente la única manera de garantizar que las mediciones físicas y digitales sean genuinas a través de la observación de múltiples fuentes y el cálculo del contexto algorítmico. La presente invención mide preferentemente además que no sólo los miembros están donde deberían estar los miembros (política, cerca geográfica, ubicación absoluta), sino que los miembros se encuentran en un contexto de proximidad apropiado, tal como en frente de la pantalla del cajero automático (ATM), ordenador portátil o quiosco de dos métodos diferentes y medios de interrogación: físico y digital.

El servidor 218 preferentemente calcula además la primera firma algorítmica 240 basada en la observación adicional y el llenado de la primera plantilla 232 después del consumo por parte del dispositivo 210 del objeto 238/segunda plantilla 235 y cualquier entrega opcional de cualquier factor fuera de banda al usuario principal, como se muestra en la Figura 2, novena etapa 9.

El servidor 218 preferentemente calcula la primera firma algorítmica final 240 y se deshace de la primera plantilla 232 y todos los factores contextuales. Preferentemente, no se almacenan en el servidor 218 factores discretos no sustitutos, desafíos, respuestas, pares clave-valor, o datos de identificación personal, ni salen del servidor 218 ni viajan a través del canal de usuario 222; el canal del sistema central 224; y el canal inteligente 226 como se muestra en la Figura 2, décima etapa 10.

Opcionalmente, el usuario principal 205 puede introducir en la aplicación 220 en el dispositivo 210 cualquier dato fuera de banda entregado antes o actualmente, tales como desafíos y respuestas, transmitidos a través del canal fuera de banda 228 desde el sistema central 215 o el servidor 218. La aplicación 220 puede procesar adicionalmente la segunda firma algorítmica 243 mediante el uso de la segunda plantilla 235. Si se configura y realiza por el usuario principal 205, el dispositivo 210 o la aplicación 220, la segunda firma 243 preferentemente modifica además los factores personales en tiempo real adicionales, los factores de comportamiento, los factores de ubicación y los factores del dispositivo basado en el comportamiento, la ubicación o la personalización del usuario, como se muestra en la Figura 2, undécima etapa 11.

A continuación, la aplicación 220 calcula preferentemente la firma algorítmica final de la segunda firma 243 y se deshace de la segunda plantilla 235 y todos los factores en la memoria, como se muestra en la Figura 2, duodécima etapa 12. Preferentemente, no se almacenan en, ni alguna vez salen del dispositivo 210, ni viajan a través del canal de usuario 222, el canal del sistema central 224 o el canal inteligente 226, factores discretos no sustitutos, desafíos, pares clave-valor o datos. El usuario principal 205 preferentemente además no es responsable del reconocimiento, recuperación, entrada, posesión, conciencia, exposición, control o conocimiento de cualquiera y todos los factores excepto por los factores fuera de banda opcionales.

A través del canal de banda inteligente triangulado 226, el servidor 218 y la aplicación 220 en el dispositivo 210 preferentemente se calcula o compara la primera firma creada a propósito 240 y la segunda firma 243, respectivamente, para la verificación algorítmica mutua, como se muestra en la Figura 2, decimotercera etapa 13. La primera firma 240 y la segunda firma 243 pueden ser de masas, estructuras y formatos iguales, similares o diferentes. Además, la comparación y evaluación de las firmas algorítmicas puede incluir, pero no se limita a: la igualdad, la congruencia, el complemento, la correlación, el enmascaramiento, el desafío-respuesta, la suma, el cálculo o cualquier otro resultado algorítmico esperado o real.

Si puede lograrse la verificación de contexto algorítmico mutua (*es decir*, la segunda firma es esencialmente idéntica o sustancialmente similar a la primera firma), la decisión de verificación de contexto total 245 se autentica, y el usuario principal 205/dispositivo 210 y el sistema central 215 generalmente se verifican de manera mutua por la aplicación 220 y el servidor 218, como se muestra en la Figura 2, decimocuarta etapa 14.

Por otro lado, si no puede lograrse la verificación de contexto algorítmico mutua (*es decir*, la segunda firma 243 no es idéntica o sustancialmente similar a la primera firma 240) por la razón que sea, entonces la decisión de verificación de contexto 245 no se autentica, y el usuario principal 205/dispositivo 210 y el sistema central 215 preferentemente no se

verifican de manera mutua por la aplicación 220 y el servidor 218, como se muestra en la Figura 2, decimoquinta etapa 15.

Preferentemente, el servidor 15 informa simultáneamente a la aplicación 220 en el dispositivo 210 el estado de la decisión de verificación de contexto 245 a través del canal inteligente 226, y al sistema central 215 a través del canal del sistema central 224, como se muestra en la Figura 2, decimosexta etapa 16.

Todos los componentes, factores, procesos, canales, sesiones y datos de autenticidad de contexto, y la decisión de verificación de contexto 245 y los algoritmos preferentemente se destruyen y eliminan de la memoria y cualquier área del servidor 218, la aplicación 220 en el dispositivo 210 y el sistema central 215. Además, los canales de conexión del canal del sistema central 224 y el canal inteligente 226 preferentemente se descartan; la aplicación 220 preferentemente se cierra; y preferentemente nada se escribe, siembra o deja atrás en el proceso, como se muestra en la Figura 2, decimoséptima etapa 17.

Opcionalmente, el sistema central 215 y/o el dispositivo 210/usuario principal 205 pueden proceder con las acciones apropiadas basadas en los resultados de la decisión de verificación de contexto 245, solos o en combinación con otros procesamientos, resultados, decisiones o estados no incluidos en la invención, como se muestra en la Figura 2, decimoctava etapa 18.

Opcionalmente, el servidor 218 reprocesa y actualiza el algoritmo de perfil 230 en la nube en base a los resultados del procesamiento de la decisión de verificación de contexto 245, en el caso de una primera sesión de inscripción o una actualización autoritaria para el algoritmo de perfil. A diferencia de los enfoques multifactoriales o de identidad tradicionales, nada literal se almacena preferentemente en el almacenamiento de datos de extremo posterior que puede identificar o recordar a un usuario; sólo un algoritmo parcial que se aplica a las observaciones de factores reales para validar o invalidar la autenticidad y la correlación de las entradas de contexto de autenticación resultantes.

La Figura 3 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra las funciones y etapas entre un sistema central, usuario, dispositivo, y la aplicación a aplicación desde dentro del dispositivo. Como se muestra en la Figura 3, una modalidad del sistema y método de autenticación de contexto de seguridad móvil 301 incluye preferentemente: un usuario principal 205; un dispositivo 210; una presentación 213; un sistema central 215; un servidor 218; una aplicación 220; un canal de usuario 222; un canal del sistema central 224; un canal inteligente 226; un canal fuera de banda 228; un algoritmo de perfil 230; una primera plantilla 232; una segunda plantilla 235; un objeto 238; una primera firma 240; y una segunda firma 243. La Figura 3 muestra además las etapas 1, 2, 3, 4, 4a, 5, 6, 7, 7a, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 de esta modalidad del sistema y método de autenticación de contexto de seguridad móvil 301.

La Figura 3 muestra además que las etapas 1, 2, 3, 4, 4a, 5, 6, 7, 7a, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 de la Figura 3 son sustancialmente similares a las etapas de la Figura 2. Sin embargo, a diferencia de la etapa 6 de la Figura 2, donde el objeto 238 se envía de la presentación 213 al dispositivo 210 (*p. ej.*, visualizar o emitir el objeto 238 al dispositivo 210), la etapa 6 de la Figura 3 ocurre preferentemente cuando el objeto 238 se transmite o envía de aplicación a aplicación. El objeto 238 se consume preferentemente por el usuario principal 205 en el dispositivo 210 a través del escaneo, detección, clic o ingreso manual del objeto 238 en forma de programa con la aplicación 238. (transferencia aplicación a aplicación, dentro del dispositivo), como se muestra en la Figura 3, sexta etapa 6.

EJEMPLOS

Los siguientes son ejemplos de diversas modalidades de la invención con el fin de ayudar a proporcionar una comprensión completa de diversos aspectos de una o más modalidades de la invención. Aunque se describen múltiples modalidades, la invención es capaz de modificaciones en diversos aspectos obvios, todo ello sin apartarse del alcance de la presente invención. En consecuencia, los siguientes ejemplos deben considerarse como de naturaleza ilustrativa y no restrictivos.

Ejemplo 1. El usuario principal 205 preferentemente se registra en un sitio web en un ordenador de escritorio o portátil con un número de identificación de usuario o mediante un servicio de inicio de sesión único (*p. ej.*, Twitter®, Facebook®, etc.). Después de iniciar sesión, el sistema central 215 puede llamar al servidor 218 mediante programación y se le devuelve un objeto personalizado, tal como un código QR. Al usuario principal 205 típicamente se le presenta el objeto en la pantalla o navegador del sitio web. El usuario principal 205 preferentemente abre y activa su iPhone®, un dispositivo móvil (*es decir*, el dispositivo 210), escanea o detecta el objeto o código en la pantalla. El objeto o código preferentemente activa la aplicación de la invención móvil 220 para contactar al servidor a través del canal secundario, y ambos típicamente comienzan a interrogarse mutuamente entre sí, el sitio, la sesión y el contexto y preferentemente calculan algorítmicamente las firmas de un solo uso (*es decir*, la primera firma 240, la segunda firma 243). Mediante el uso del GPS y la ubicación IP, el servidor 218 y la aplicación 220 del dispositivo generalmente miden la ubicación del objeto original en la pantalla (*es decir*, el objeto 238) y la ubicación del usuario principal 205 y el dispositivo 210 para el cálculo absoluto y de proximidad. Estos factores se aplican preferentemente de manera algorítmica en cada extremo de la firma. Tras la verificación mutua de esas firmas por la aplicación móvil 220 y el servidor 218, la decisión de autenticación se alcanza preferentemente y el estado (*es decir*, la decisión de verificación de contexto 245)

generalmente se comunica a todas las partes. El resto del procesamiento se maneja de forma pasiva sin la participación del usuario o el conocimiento, la interrogación o el desafío/respuesta. El usuario principal 205, luego es generalmente libre de entrar en el sitio que se le ha dado permiso por el sitio basado en un estado de autenticación positivo, o denegado basado en uno negativo. Como tal, se logra preferentemente una autenticación de contexto de múltiples factores definitiva.

Ejemplo 2. El usuario principal 205 abre una aplicación de juegos en su dispositivo móvil Android®. Desde dentro de la aplicación de juegos, se llama a la aplicación 220 en el dispositivo 210 a través de una API interna del dispositivo (una interfaz de programación de aplicaciones llamada un gestor de protocolos en este caso). Preferentemente, no se requiere de manera general un código, escaneo o entrada manual. El enlace de la sesión se pasa generalmente del juego a la aplicación 220 a la perfección a través del gestor de protocolos-*es decir*, dando la vuelta de una forma aplicación a aplicación. Tras el inicio de esa aplicación 220, la ubicación y el comportamiento del usuario principal 205 (orientación del dispositivo 210) se miden junto con las credenciales estándares correspondientes y se aplican algorítmicamente a las firmas en cada lado (*p. ej.,* la primera firma 240 y la segunda firma 243). Generalmente, ningún dato discreto se envía más allá del dispositivo o servidor, aparte de las firmas resultantes. En este caso, generalmente se encuentra que las firmas (la segunda firma 243 y la primera firma 240) no coinciden o se correlacionan. Por lo tanto, el usuario principal 205 típicamente no puede autenticarse y generalmente se le niega el acceso al juego. Bajo lo técnico, es preferible porque el usuario principal 205 se encuentra en un país no autorizado para jugar ese juego, pero ni este detalle ni la capacidad para evadir su ejecución se exponen al usuario principal 205, la red o la sesión. La protección de seguridad típicamente se logra a través de la autenticación consciente del contexto.

Ejemplo 3. El usuario principal 205 inicia sesión en un sitio (sistema central 215 en la presentación 213) como en el primer ejemplo, pero desde un dispositivo móvil completamente nuevo (*es decir*, el segundo dispositivo), no reconocido o registrado previamente. El usuario principal 205 típicamente escanea la pantalla después de iniciar sesión y falla la autenticación (*es decir*, la segunda firma 243 no coincide con la primera firma 240) debido a malas credenciales de factores del dispositivo. Luego se presentan al usuario factores privados fuera de banda con un desafío de una sola vez, enviados fuera de banda (a través de un Tweet® privado de Twitter®, por preferencia) que el usuario principal 205 ingresa preferentemente en la aplicación del dispositivo móvil (*es decir*, la aplicación 220) en el segundo dispositivo. Esta entrada se sintetiza con el resto de los factores de la segunda plantilla 235 para crear una segunda firma modificada. La segunda firma modificada preferentemente se vuelve a comparar con la primera firma recién modificada, privada del desafío personalizado enviado, y ambas firmas modificadas coinciden ahora, lo que permite la autenticación de contexto exitosa, y la actualización inmediata de los factores de datos adicionales del segundo dispositivo de vuelta en el servidor 218. Preferentemente, no se tuvo que enviar ningún dispositivo literal a través del canal inteligente 226 y el usuario se autenticó rápidamente, en general, en el contexto. En este caso, el servidor de la invención 218 instancia del algoritmo de perfil 230 se actualiza preferentemente debido a la modificación del nuevo dispositivo bendecido.

Estos ejemplos son meramente ilustrativos y no se limitan a las opciones y posibilidades totales de aplicar esta invención a tecnologías y capacidades alternativas, nuevas y emergentes con respecto a requisitos, limitaciones, oportunidades y modalidades de verificación y autenticación de contexto del servidor, usuario, dispositivo o sistema central.

Información adicional

La primera plantilla 232 y la segunda plantilla 235 son preferentemente desechables, creadas a propósito, sustitutas, específicas del contexto y dinámicas en masa (*es decir*, tamaño, secuencia, formato, estructura, profundidad y cantidad de registros) cuya composición y algoritmo de llenado se definen generalmente por el contexto y el procesamiento de miembros. La decisión de verificación mutua por parte del servidor 218 y el dispositivo 210 generalmente se logra algorítmicamente, no mediante un proceso de "búsqueda y coincidencia" basado en información de referencia estática, fija o reutilizable. Ni la primera plantilla 232 ni la segunda plantilla 235 es la autoridad de coincidencia para la otra (u otras en el caso de muchas). La decisión de verificación de contexto 245 de las firmas de plantilla (*es decir*, la primera firma 240 y la segunda firma 243) generalmente se logra matemáticamente o no. Preferentemente, los resultados detallados de la decisión de verificación de contexto 245 o su anticipación no pueden calcularse o conocerse por el servidor 218 o el dispositivo 210 por adelantado hasta que el servidor 218 o el dispositivo 210 ingresen en la sesión de contexto de procesamiento con todos los miembros presentes basados en las plantillas generadas por algoritmo de perfil.

Generalmente, el algoritmo de perfil 230 es el elemento persistente del procesamiento del servidor 218 que representa un contexto único de un usuario, dispositivo, sitio, sesión, comportamiento, ubicación, proximidad y factores de personalización. Cada contexto preferentemente tiene un algoritmo único almacenado en la nube del servidor generado en el primer registro o al que se hace referencia tras la autenticación posterior para la generación de plantillas y el procesamiento resultante. En el uso normal, el algoritmo de perfil 230 se usa para generar dos plantillas (como se muestra en la Figura 2, etapa 3) cuando el sistema central 215 lo solicita para autenticar el contexto del usuario principal 205/dispositivo 210. La primera plantilla 232 destinada para el procesamiento por el servidor 218 es generalmente más completa mientras que la segunda plantilla 235 para el consumo de la aplicación 220/dispositivo 210 es generalmente menos completa. Sin embargo, tanto la primera plantilla 232 como la segunda plantilla 235 se basan generalmente en el algoritmo de perfil 230 sembrado matemáticamente usado para afirmar la correlación más tarde durante el

procesamiento de la decisión de verificación de contexto 245, ya que tanto la primera plantilla 232 como la segunda plantilla 235 se modulan por la entrada e influencia de factores dinámicos y aleatorios, lo que resulta en firmas de decisión potencialmente correlativas. El algoritmo de perfil 230 se usa entonces preferentemente para procesar la primera firma 240 y la segunda firma 243 para determinar la correlación tanto por la aplicación 220/dispositivo 210 como por el servidor 218 para la autenticación mutua sin requerir una única búsqueda o coincidencia autoritaria. Todas las decisiones de componentes procesadas por la decisión de verificación de contexto 245 generalmente se crean con un propósito y son matemática y universalmente únicas. El enfoque de la presente invención es revolucionario con respecto a los métodos existentes, ya que los métodos existentes se basan en la coincidencia de patrones simple o la distribución, custodia y mantenimiento persistente de claves públicas/privadas. El sistema y método de autenticación de contexto de seguridad móvil de la presente invención, sin embargo, preferentemente permite el uso de múltiples dispositivos sin la distribución de claves, la inscripción automática en el primer uso, y la capacidad para procesar factores, comportamientos y contextos infinitamente medibles. Además, a diferencia de los métodos y esquemas de autenticación de seguridad convencionales, el sistema central 215, el usuario principal 205, o los factores del dispositivo, algoritmos o firmas no están federados en el servidor 218 para evitar la administración de contexto cruzado y la asociación del riesgo de privacidad. Si bien los métodos de autenticación de seguridad existentes y convencionales pueden utilizar dicha federación como una característica o beneficio, la presente invención considera la federación de contexto como una responsabilidad. Como tal, la asociación del riesgo de privacidad generalmente debe gestionarse, aplicarse y verificarse (independientemente de la invención) y generalmente no aumenta la facilidad de uso, solidez o seguridad de la presente invención.

Generalmente, la presente invención no permite reutilizar o enviar los datos discretos entre las capas de procesamiento interno o los canales de comunicación externos de una forma no sustitutiva, no sintetizada. Adicionalmente, ningún par de valores de clave de datos generalmente viaja a través del mismo canal de transmisión. Los desafíos y las respuestas generalmente no viajan a través del mismo canal de transmisión en la misma dirección (*es decir*, el canal de usuario 222, el canal del sistema central 224, y el canal inteligente 226) y ningún dato discreto generalmente sale de la capa interna en la que se observó o interrogó la capa interna.

Todo el proceso de decisión de verificación de contexto 245 generalmente se triangula e interrumpe entre el sistema central 215, el servidor 218, y el dispositivo 210/usuario principal 205 a través de los canales encriptados, el canal de usuario 222, el canal del sistema central 224 y el canal inteligente 226 (y opcionalmente el canal fuera de banda 228). Preferentemente, ningún identificador no sustituto con relación al sistema central 215, el dispositivo 210 o el usuario principal 205 se transmite solo o en pares clave-valor. Los valores de los factores aleatorios generalmente se aplican algorítmicamente a cada valor de plantilla en lugar de transmitirse, inspeccionarse o identificarse literalmente.

El proceso de comparación de firmas resultante de la decisión de verificación de contexto 245 generalmente aplica el algoritmo de perfil a través del espectro de todos los valores posibles y fácticos de los factores de múltiples masas entre la primera firma 240 y la segunda firma 243 para lograr la verificación de contexto sin la identificación, búsqueda o coincidencia de factores individuales. Este procesamiento unidireccional preferentemente logra la correlación o no correlación de la decisión de verificación de contexto, pero nunca la asociación o definición, en base al algoritmo de perfil.

Los datos de autenticación y procesamiento de contexto preferentemente fluyen de manera simultánea y bidireccional a través del canal de usuario encriptado 222, el canal del sistema central 224 y el canal inteligente 226, asegurando así la inmunidad de la interceptación, correlación, repetición o previsibilidad. A diferencia de los sistemas descritos en las referencias existentes, que transmiten el flujo de datos seguros en una dirección de fuente a autoridad, a través del sistema central 205, la presentación 213 y el dispositivo 210 a un servidor equivalente 218 para la inspección/comparación (a menudo como un par clave-valor codificado, encriptado u ofuscado), la presente invención preferentemente separa y bifurca ese flujo sustituto por diseño como un método para una interrogación, medición, integridad, análisis e inmunidad de compromiso más mutuos, seguros, privados y efectivos.

El sistema central 205, el servidor 218, y el usuario principal 205/dispositivo 210 son preferentemente miembros de una fórmula de contexto de autenticación interdependiente que se aleja del modelo tradicional de cliente-servidor, de secreto compartido. A diferencia de los métodos existentes, normalmente no hay autoridad persistente (búsqueda de datos y comparación/coincidencia) en la presente invención. Sólo a través de la presencia y participación activa de todos los miembros y el interrogatorio en múltiples perspectivas de cualquiera o todos los factores, la decisión de verificación de contexto 245 puede ser mutuamente acordada. Todos los factores influyen meramente y de manera típica en los algoritmos de autenticación y, por lo tanto, normalmente modifican las firmas resultantes para la autenticación mutua, en lugar de transmitir en su totalidad o en parte para una comparación autoritaria eventual contra un valor de referencia almacenado y recuperado. Esta separación de preocupaciones en la presente invención es novedosa, contextual, interdependiente y de fuerte innovación con respecto a la autenticación y privacidad de contexto.

La transmisión y la modalidad del objeto 238 (a través de la presentación 213) pueden realizarse mediante cualquier método o modo requerido o soportado por la transmisión técnica y las oportunidades de consumo o las limitaciones del sistema central 215 y el dispositivo 210, a través del canal de usuario 222, el canal del sistema central 224, y el canal inteligente 226. Estas áreas conceptuales generalmente se conocen por los expertos en la técnica y típicamente se cubren por las referencias existentes; y se emplean meramente para soportar una transmisión exitosa y efectiva máxima

del objeto 238 en muchos contextos diversos. Los ejemplos de dichas modalidades para la transmisión del objeto 238 incluyen, pero no se limitan a: (1) el enlace de imagen visual, etiqueta, video o código QR presentado por un navegador, pantalla u objeto imprimible, escaneado por un dispositivo informático electrónico móvil con tales capacidades; (2) la señal audible transmitida y detectada por un dispositivo informático móvil desde una fuente; (3) la transmisión textual, visual, audible o programática a través de SMS, MMS, correo electrónico, Tweet®, mensaje directo, chat, hipervínculo del navegador, aplicación, pantalla, transmisión físicamente impresa o visualmente codificada a un dispositivo informático móvil; (4) la transmisión codificada de campo cercano (NFC) transmitida y consumida por un dispositivo informático móvil; (5) la transmisión y consumo sensorial de comportamientos tales como gestos, sacudidas del dispositivo, movimiento, aceleración, proximidad u otros mecanismos de estímulo/respuesta; (6) el intercambio de datos de interfaz programática tal como RPC, API, proceso en memoria, búsqueda en base de datos, pulso, código de tiempo, comunicación oculta o entre procesos; (7) la entrada manual o por gestos de los datos recibidos o deducidos de la transmisión oral, escrita, dramática, musical, visual, emocional, histórica, interpretativa u otra transmisión no informática; y (8) cualquiera o todo lo anterior transmitido, recibido y consumido ya sea dentro de banda o fuera de banda, con o sin la asistencia de tecnología intermediaria, humanos, símbolos o idioma.

El uso de códigos QR en la presente invención, a diferencia de todos los métodos existentes, se utiliza meramente para su propósito principal de simplemente transmitir un enlace localizador universal de recursos (URL) a la aplicación 220 en el dispositivo 210 a través del escaneo y la decodificación, el enlace, la entrada o el procesamiento. Los métodos convencionales generalmente se basan en el uso de códigos QR para integrar, codificar o encriptar información secreta de sesión, sitio web, usuario o desafío para decodificarse y luego emparejarse con los factores de dispositivo o usuario y enviarlos conjuntamente al servicio de extremo posterior para la identificación. Cuando se usa, la presente invención evita la sobrecarga del código QR y simplemente se basa en el código QR para su propósito abierto y libre de patentes deseado *es decir*, proporcionar un método elegante y utilizable para transmitir un URL o un objetivo de sesión desde la pantalla de la presentación 213 a la aplicación móvil 220 a través del escaneo óptico por la cámara del dispositivo 210 y decodificar mediante la aplicación 220.

Todos los factores de múltiples masas pueden ser cualquiera o todos los factores contextuales que pueden cuestionarse, interrogarse, detectarse, inferirse, realizarse, medirse inmediata o históricamente por un miembro más, individualmente o en combinación con otros factores o miembros, desde una o más perspectivas y trayectorias de canales, en una o más ocasiones durante el ciclo de vida de la sesión o a través de varias sesiones. La presente invención preferentemente asume una firma de múltiples masas (la firma del servidor 240/la segunda firma 243) basada en una interrogación y un llenado de plantillas generadas por algoritmos de perfil de uno a muchos factores de contexto individuales que incluyen, sin limitación: (1) características, atributos o contexto del servidor, dispositivo, sesión, red o usuario; (2) ubicación, proximidad o límites del miembro, dispositivo, presentación o red; (3) ubicación o movimiento fijo, original, definido, proximal, relacional, absoluto o móvil; (4) comportamiento del usuario o dispositivo, gesto, estadísticas, orientación, rendimiento, respuesta o patrón; (5) desafío/respuesta, comportamiento del usuario "ludificado", prueba, habilidad, actividad, recuerdo o reconocimiento; (6) análisis histórico de datos, estadísticas, comportamiento, contexto, ubicación, proximidad o movimiento; (7) desafíos y respuestas individuales de texto, imágenes, cadenas, frases, palabras, PIN, números; y (8) otros factores habilitados o soportados por la tecnología o procesamiento del sistema central emergente 215, el dispositivo 210 o el servidor 218.

Ejemplos de tales factores pueden ser que el usuario principal 205 se autentique con éxito con todas las credenciales normales cuando el usuario principal 205 sostiene el dispositivo móvil 210 en modo vertical orientado hacia el norte. Estos comportamientos y ubicaciones actúan como entradas de factores de múltiples masas al procesamiento algorítmico de la primera plantilla 240 y la segunda plantilla 243 para llegar a la decisión de la firma. Cualquier otra orientación afectaría y generaría una firma no válida, pero no revelaría la naturaleza o la causa del fallo a la red, al usuario o a un hacker.

Otro ejemplo puede ser la medición histórica de la ubicación del usuario principal 205/dispositivo 210, movimiento o incluso locomoción (marcha andante, altura de referencia llevada por el dispositivo, intervalo de locomoción, etc.) a lo largo del tiempo. Si, tras la autenticación, esos factores estaban desproporcionados con el uso histórico normal, de cualquier otra manera las credenciales aceptables típicamente caerían fuera de contexto (firma) o tal vez desencadenarían un rigor fuera de banda adicional para verificar. Sin embargo, las credenciales no se usan ni se inspeccionan físicamente o transmiten de una manera que identifiquen individualmente al usuario de una forma no privada e inmutable.

La autenticación mutua y la decisión de verificación de contexto 245 se diseñan preferentemente con el fin de permitir que el sistema central principal 215 o el usuario principal 205/dispositivo 210 acceda, autorice, ingrese, envíe, verifique, confirme, presente, descargue, transmita, compre, modifique, elimine, cancele o de cualquier otra manera interactúe con los privilegios apropiados cualquier sesión, recurso, datos, ubicación física/virtual, contenido, bienes, servicios, medios, experiencias, conexiones, logros, mensajes, etc., ya sea sólo por sus méritos (aprobado/no aprobado) o en combinación con otras decisiones de verificación de contexto 245 o métodos, credenciales o decisiones preexistentes, paralelos o posprocesados, nativos o externos, de identidad o autenticación. La decisión de verificación de contexto 245 puede basarse además en el procesamiento de uno o más sistemas centrales, usuarios, dispositivos y plantillas para todos los factores en aislamiento, secuencia o contexto de combinación. Por ejemplo, donde no existe el sistema central 215, todo el proceso de decisión de verificación de contexto 245 puede ocurrir entre el primer usuario/primer dispositivo, el

segundo usuario/segundo dispositivo y el servidor 218 para proporcionar decisiones de verificación de contexto de igual a igual. Otro ejemplo puede ser cuando múltiples combinaciones de usuario/dispositivo contra un único sistema central 215/servidor 218 se verifican contextualmente para autenticar y desbloquear conjuntamente un recurso o activo común en el sistema central 215.

Como se muestra en la Figura 2, el canal de usuario 222, el canal del sistema central 224, el canal inteligente 226 (y el canal fuera de banda 228) pueden incluir canales y tecnologías de comunicación homogéneos o heterogéneos, flujos direccionales, medios de transmisión (encriptados o no), mediados por humanos o digitalmente, por proxy o directos, en tiempos simultáneos o escalonados, o tiempo de vida (TTL). El canal de usuario 222 puede ser tradicionalmente una conexión web entre el sistema central 215 y el dispositivo de visualización del usuario final (la presentación 213 o el dispositivo 210 en el caso de la navegación/aplicación en el dispositivo móvil). El canal del sistema central 224 puede ser una conexión privada entre el sistema central 215 y el servidor 218. El canal inteligente 226 es preferentemente una segunda conexión privada entre el servidor 218 y el dispositivo 210 del usuario principal 205. El canal fuera de banda 228 preferentemente representa un canal adicional opcional entre cualquiera de los siguientes: (1) el sistema central 215 y/ el usuario principal 205/dispositivo 210; o (2) el servidor 218 y el usuario principal 205/dispositivo 210, tales como correo electrónico, SMS, chat o llamadas de voz para entregar datos o factores fuera de banda únicos al usuario para su uso dentro del flujo de la invención.

Preferentemente, en ningún momento las plantillas, las decisiones de verificación de contexto, los factores o los canales son capaces de o se usan para el propósito de identificar, exponer o registrar la identidad del usuario principal 205 o el dispositivo 210 en el proceso, sólo para autenticar y verificar el contexto contra los contextos previamente verificados. Un ejemplo de esto sería el enfoque convencional de registrar la dirección IP de los puntos finales del sistema central 215 o el dispositivo 210 de cualquier canal equivalente (p. ej., el canal de usuario 222, el canal del sistema central 224, el canal inteligente 226 y el canal fuera de banda 228). La presente invención simplemente usa de manera típica estas entradas para modificar el algoritmo y el efecto resultante sobre la firma de la plantilla, un enfoque evidentemente innovador y más robusto, seguro y privado.

Preferentemente, los únicos datos del usuario principal 205/dispositivo 210 que persisten en el servidor 218 son los algoritmos de perfil usados para procesar los factores del dispositivo y los factores de personalización (*es decir*, comportamiento, ubicación, proximidad, personalización) en una forma algorítmica no asociativa que alimenta la composición y el procesamiento de la primera plantilla 232. Preferentemente, el servidor 218 no puede usar el algoritmo de perfil, los factores de dispositivo o los factores de personalización de manera repetida o predictiva para identificar un usuario, dispositivo, sesión, ubicación o contexto en cualquier momento antes o después de una sesión activa. Más bien, el servidor 218 sólo puede servir para proporcionar entradas en el procesamiento y la modificación en tiempo real de la primera plantilla 232 dentro de la sesión activa que eventualmente conduce a un resultado mutuamente verificado-*es decir*, la decisión de verificación de contexto 245, con el procesamiento realizado en tiempo real en el dispositivo 210 tras la creación y comparación de la segunda plantilla 235.

Los datos de la decisión de verificación de contexto 245 generalmente no se almacenan, persisten o recuperan desde el dispositivo 210 o el usuario principal 205. Preferentemente, todos los factores almacenados dentro del dispositivo 210/usuario principal 205 se interrogan, consultan, detectan o solicitan dinámicamente en tiempo real mediante la aplicación 220, se procesan en la segunda plantilla 235 (y eventualmente la segunda firma 243), e inmediatamente se disponen desde la memoria. Generalmente, no se transmiten todos los factores discretos desde el dispositivo 210/usuario principal 205 fuera del dispositivo 210 a través del canal de usuario 222/canal del sistema central 224/canal inteligente 226 en cualquier momento. A diferencia de los métodos de autenticación convencionales, la presente invención preferentemente no se basa en cookies, certificados o claves públicas-privadas persistentes sembradas, almacenadas o referenciadas, sobre el dispositivo.

La triangulación de la ubicación entre el sistema central 215, el dispositivo 210 y el servidor 218 generalmente se realiza a través de una síntesis de la línea de visión, sonido ambiental o vibración/movimiento/sensación directa o física y la información digital obtenida de la tecnología consciente de la ubicación, que incluye, sin limitación: GPS, código de transmisión, mapeo de IP a ubicación, verificación óptica de un campo o perspectiva visual común universalmente único, verificación audible de un ambiente o perspectiva acústica común (mostrado en la Figura 6). Por ejemplo, el factor de ubicación se calcula preferentemente tanto por el servidor 218 como por la aplicación 220 en el dispositivo 210 a través de una síntesis triangulada de múltiples perspectivas de los datos de ubicación física y digital del sistema central 205, la presentación 213/objeto 238, y el dispositivo 210 en el punto de entrega, presentación, consumo, procesamiento y mensajería en relación con el servidor 218. Preferentemente, ninguna fuente única de datos de factores de ubicación se considera autoritaria, tal como con la decisión de verificación de contexto 245 en sí. Preferentemente, todos los componentes se alinean o igualan, o el contexto no puede verificarse.

Aunque la descripción escrita anterior de la invención permite a un experto en la técnica hacer y usar lo que actualmente se considera el mejor modo de la misma, los expertos en la técnica entenderán y apreciarán la existencia de variaciones, combinaciones y equivalentes de la modalidad, método y ejemplos específicos en la presente descripción. Por lo tanto, la invención no debería limitarse por la modalidad, el método y los ejemplos descritos anteriormente, sino por todas las modalidades y métodos dentro del alcance de la invención como se reivindica.

Parte 2 - ludificación

La Figura 4 es un diagrama de flujo de bloques funcional de una modalidad del proceso de ludificación del sistema y método de autenticación de contexto de seguridad móvil y muestra las etapas iniciales del proceso de ludificación-*es decir*, seleccionar y configurar los factores contextuales tales como los factores de ubicación, los factores de comportamiento y los factores de personalización. Como se muestra en la Figura 4, una modalidad del sistema y método de autenticación de contexto de seguridad móvil 301 incluye preferentemente: un usuario principal 205; un dispositivo 210; un servidor 218; una aplicación 220; un canal inteligente 226; y un algoritmo de perfil 230. La Figura 4 muestra además las etapas 100, 200, 300, 400 de una modalidad del proceso de ludificación 401 del sistema y método de autenticación de contexto de seguridad móvil 401.

La ludificación de la presente invención, preferentemente se refiere a la introducción del comportamiento del usuario, características, técnicas de diseño de comportamiento y/o estilo del usuario para el proceso de autenticación. El proceso de ludificación de la invención se usa preferentemente en una o más aplicaciones y procesos para mejorar el proceso de autenticación.

La Figura 4 muestra la primera etapa 100 del proceso de ludificación, dentro del contexto de un inicio de sesión normal del usuario, acceso, o verificación de contexto de autenticación a través de la aplicación 220 en el dispositivo 210 al sistema central 215 en la presentación 213. Específicamente, como se muestra en la Figura 4, el usuario principal 205 puede afectar, controlar y fortalecer el procesamiento de la segunda plantilla 235 para la segunda firma 243 a través de la aplicación 220. Específicamente, el usuario principal 205 puede fortalecer el procesamiento de la segunda plantilla 235 para la segunda firma 243 mediante la incorporación, configuración y/u operación de los factores personales del usuario o dispositivo: (1) comportamiento; (2) ubicación; y (3) factores de personalización.

Estas restricciones de procesamiento pueden ser superiores a lo que puede requerir el sistema central 215 o el servidor 218, lo que proporciona al usuario principal 205 control y personalización. Como resultado, típicamente se produce una fortaleza, privacidad y robustez adicionales de la verificación del contexto de autenticación.

Durante el proceso de registro *R1*, como se muestra en la segunda etapa 200 en la Figura 4, el usuario principal 205 realiza preferentemente el procesamiento de la segunda plantilla 235 para la segunda firma 243. Esto puede realizarse por el usuario principal 205 seleccionando, habilitando, comprando, configurando y/o realizando el procesamiento para interrogar y procesar cualquiera o todos los factores de usuario (a través de la compra en la aplicación y los controles dentro de la aplicación 220 en el dispositivo 210): los factores personales 405 constan de: (1) factores de comportamiento 410 (*es decir*, algo que el usuario o dispositivo hace o puede hacer); (2) factores de ubicación 413 (*es decir*, algún lugar en el que el usuario o dispositivo se encuentra o está relacionado); o (3) factores de personalización 415 (*es decir*, factores de personalización de conocimiento, preferencia, habilidad o posibilidad).

A continuación, la tercera etapa 300 de la Figura 4 muestra que, durante el proceso de registro *R1* mediante la aplicación 220, los factores de comportamiento 410, los factores de ubicación 413 y los factores de personalización 415 generalmente se interrogan junto con los factores múltiples estándar por la política del usuario principal 205 o la configuración. El llenado de la segunda plantilla 235 y el procesamiento de la primera firma 240 generalmente se afectan por estos factores y ese procesamiento algorítmico normalmente se transmite al servidor 218 y se registra como una actualización al algoritmo de perfil (junto con los factores de dispositivo estándar) para usar en el futuro la primera plantilla del servidor 232 para la generación y procesamiento de la primera firma 240.

La Figura 4 muestra la cuarta etapa 400 del proceso de ludificación 401 donde los factores personales 405 se calculan como parte de la segunda plantilla 235. Específicamente, los subcomponentes de comportamiento, ubicación y personalización del algoritmo de factores personalizados preferentemente no se transmiten al servidor 218 en forma discreta, sino que preferentemente se calculan como parte de la segunda plantilla 235 durante el primer registro en forma algorítmica. El algoritmo de factores personalizados se añade preferentemente al procesamiento de la segunda plantilla 235 para la segunda firma 243 (junto con los factores del dispositivo), pero solo no contiene ni revela factores de comportamiento literal o de identificación 410, factores de ubicación 413, factores de personalización 415 o datos. Generalmente, el uso de los factores fuera de banda junto con un nuevo registro (*es decir*, registros posteriores) puede actualizar el algoritmo de perfil en el servidor 218.

La Figura 5 es un diagrama de flujo de bloques funcional de una modalidad del proceso de ludificación del sistema y método de autenticación de contexto de seguridad móvil y muestra las últimas etapas del proceso de ludificación-*es decir*, procesar la primera plantilla por el servidor y la segunda plantilla por la aplicación del dispositivo. Como se muestra en la Figura 5, la quinta etapa 500 de una modalidad del proceso de ludificación ocurre cuando la aplicación 205 procesa la segunda plantilla 235 para crear la segunda firma 243. En particular, durante el proceso de autenticación siguiente, el usuario principal 205, la aplicación 220 o el dispositivo 210 procesa la segunda plantilla 235 para crear la segunda firma 243 interrogando preferentemente el "rendimiento" o la "interrogación" de los factores personales 410 *(es decir,* comportamientos, ubicaciones, proximidades y factores de personalización) junto con el llenado de la segunda plantilla tradicional 235. La aplicación 220 a través del dispositivo 210 preferentemente detecta, interroga y captura estos factores a través de su GPS nativo, acelerómetro, capacidades de software o hardware o tecnología personalizada. La aplicación 220 preferentemente mide además la relación entre la línea de visión/detección/escaneo

físico y los datos de ubicación digital (proximidad), su ubicación absoluta, o ubicación contra otro punto fijo, dispositivo o elemento de referencia, como se muestra en la Figura 6. Con estos datos llenados en la segunda plantilla 235, la segunda firma 243 se calculará y comparará y/o correlacionará luego preferentemente con la versión del servidor 218 de la primera firma 240, a través del canal inteligente 226.

Cuando el sistema central 215 o el usuario principal 205 solicitan una decisión de verificación de contexto 245, el procesamiento de la primera plantilla 232 para la primera firma 240 se procesa preferentemente en el servidor 218 de acuerdo con los factores personales 405 que influyen en los algoritmos de perfil, como se muestra en la Figura 5, sexta etapa 600.

Luego, después del procesamiento de la segunda plantilla 235, la aplicación 220 preferentemente interroga, recrea y/o realiza las métricas reales de los factores personales 405 junto con el equilibrio de todos los factores existentes para crear la segunda firma 243, como se muestra en la Figura 5, séptima etapa 700.

Si la primera firma 240 no coincide con la segunda firma 235, la decisión de verificación de contexto 245 es preferentemente falsa o no autenticada. Por otra parte, si la primera firma 240 coincide con la segunda firma 235, la decisión de verificación de contexto 245 se considera preferentemente verdadera o autenticada, como se muestra en la Figura 5, octava etapa 800.

Alternativamente, si la primera firma 240 no es complementaria o correlativa con la segunda firma 243, la decisión de verificación de contexto 245 se considera preferentemente falsa o no autenticada. Si la primera firma 240 es complementaria o correlativa con la segunda firma 243, la decisión de verificación de contexto 245 se considera preferentemente verdadera o autenticada, como se muestra en la Figura 5, novena etapa 900.

Opcionalmente, si la primera firma 240 no coincide con la segunda firma 243 por alguna razón, el servidor 218 o el sistema central 215 puede enviar los factores fuera de banda al usuario principal 205 a través del canal fuera de banda 228 para el ingreso en la segunda plantilla 235. El servidor 218 puede hacer lo mismo con la primera plantilla 232, volver a calcular la primera firma 240/segunda firma 243 y permitir una actualización de los factores del dispositivo o los factores personales 405, o ambos, como se muestra en la Figura 5, décima etapa 1000. Esto puede ocurrir cuando se utiliza un dispositivo nuevo no reconocido; cuando los factores de ubicación cambian; o la aplicación 220 ejecuta u observa factores de comportamiento del usuario nuevos o diferentes o factores de personalización en el dispositivo 210 durante la autenticación.

Opcionalmente, el sistema central 215 puede requerir que el servidor 218 habilite todos los factores personales 405 y los factores del dispositivo desde su solicitud inicial para autenticarse a través del canal del sistema central 224, permitiendo así que la funcionalidad anterior se interrogue y procese pasivamente a través de la aplicación 220 en el dispositivo 210 con o sin permiso, conocimiento o participación intencional del usuario principal 205/dispositivo 210 para el llenado de la segunda plantilla 235 y el cálculo de la segunda firma 243, como se muestra en la Figura 5, undécima etapa 1100.

Ejemplos

Los siguientes son ejemplos de diversas modalidades de la invención con el fin de ayudar a proporcionar una comprensión completa de diversos aspectos de una o más modalidades de la invención. Aunque se describen múltiples modalidades, la invención es capaz de modificaciones en diversos aspectos obvios, todo ello sin apartarse del alcance de la presente invención. En consecuencia, los siguientes ejemplos deben considerarse como de naturaleza ilustrativa y no restrictivos.

Ejemplo 1. En este primer ejemplo, se supondrá que el usuario principal 205 preferentemente interviene en un flujo de autenticación normal contra el sistema central 215 desde el dispositivo 210, como se describe en la primera invención, y preferentemente ha seleccionado, comprado, configurado la aplicación 210 para realizar factores de comportamiento de autenticación adicionales y personalizados de rigor. Después de iniciar sesión, el proceso del usuario principal 205 preferentemente proporciona todas las credenciales válidas, pero normalmente no realiza ningún comportamiento especial. El usuario principal 205 se encuentra con un estado fallido (generalmente como resultado de una falta de coincidencia entre la segunda firma 243 y la primera firma 240 debido a la falta de factores personales, la influencia del algoritmo de factores y la modificación de la firma resultante). Al volver a intentarlo, el usuario principal 205 preferentemente mantiene el dispositivo 210 en modo vertical para escanear y puede agitar el dispositivo en un movimiento determinado (*es decir*, el comportamiento esperado). Como resultado, el usuario principal 205 se encuentra preferentemente con un estado de autenticación exitoso (*es decir*, la segunda firma 243 coincide con la primera firma 240) debido a la aplicación de la influencia apropiada del factor en el procesamiento de la firma.

Ejemplo 2. En este segundo ejemplo, el usuario principal 205 preferentemente ha preconfigurado, para protección, (a través de la compra, selección y configuración en la aplicación) la restricción de no autenticarse si el contexto es tal que su dispositivo 210 no está en la misma ubicación que la presentación 213, o su dispositivo 210 no está en el mismo lugar que cuando el usuario principal 205 se registró por primera vez (*es decir*, el primer registro). El usuario principal 205 inicia sesión, escanea el código de autenticación de la página web y no logra autenticarse, al darse cuenta de que

está en el extranjero y no en su entorno local. El usuario principal 205 lo vuelve a intentar y se le solicita un factor fuera de banda para verificar que desea añadir esta configuración regional como confiable. El usuario principal 205 recibe el factor fuera de banda por correo electrónico, lo introduce en la aplicación 220 en el dispositivo 210 y una nueva segunda plantilla modificada se calcula y compara con la primera plantilla modificada del servidor 218 proporcionado. El usuario principal 205 entonces se autentica preferentemente. Además, la versión del servidor 218 del algoritmo de perfil 230 del usuario principal 205 (específicamente a través del factor personal/factor de ubicación) se actualiza para la nueva influencia de localización para el procesamiento futuro.

Ejemplo 3. En este ejemplo, el usuario principal 205 ha configurado preferentemente la aplicación 220 con un número de identificación personal personalizado (PIN) para desbloquear la aplicación cuando se usa en el dispositivo 210. Si el usuario principal pierde su dispositivo 210, y otro usuario intenta autenticarse en contexto, sin la entrada de ese número de identificación personal, la segunda firma 243 no coincidirá con la primera firma 240, y la autenticación típicamente fallará (protegiendo así al usuario principal 205 y al dispositivo 210). El proceso generalmente no revelará por qué ocurre el fallo para garantizar que el otro usuario no gane conocimiento o información para reintentar o intentar repetir, ingeniería inversa o modificación del contexto para obtener acceso ilícito. Tras la recuperación del dispositivo 210, el usuario principal real 205 ingresa su PIN y puede reanudar la autenticación contextual adecuada y apropiada.

Estos ejemplos son meramente ilustrativos y no se limitan a las opciones y posibilidades totales de aplicar esta invención a tecnologías y capacidades alternativas, nuevas y emergentes con respecto al comportamiento, contexto, ubicación o personalización del usuario o dispositivo.

Información adicional

A pesar de infinitos valores discretos posibles o combinaciones para los factores personales o factores del dispositivo, la representación algorítmica dentro de la primera plantilla 232/segunda plantilla 235, y por lo tanto, la primera firma 240/segunda firma 243 será de preferencia universalmente única pero de un valor resuelto de profundidad predecible para el reprocesamiento por el servidor 218 o el dispositivo 210, respectivamente. Está permitido que la primera plantilla 232 y la segunda plantilla 235 (así como también la primera firma 240 y la segunda firma 243) sean de composición, profundidad, longitud y/o estructura similares o diferentes.

El efecto de los factores personales sobre la decisión de verificación de contexto 245 está completamente dentro del control del usuario principal 205, y su procesamiento es preferentemente irrelevante para el sistema central 215, que simplemente se preocupa del estado definitivo total de la decisión de verificación de contexto 245. Esto ilustra preferentemente la innovación y novedad de esta invención bajo los auspicios del usuario principal 205 con respecto al fortalecimiento, la privatización o la personalización de su contexto de autenticación a través de la aplicación 220 por encima de las demandas del servidor 218 o el sistema central 215.

Los factores personales y los factores del dispositivo preferentemente no pueden, y no identifican el usuario principal 205 o el dispositivo 210 fuera del contexto de la primera firma 240/segunda firma 243, el procesamiento de la firma de contexto y la decisión de verificación de contexto 245. Preferentemente, no son factores independientes o identificadores de usuario o dispositivo significativos en ningún aspecto.

Los factores de comportamiento pueden ser cualquiera de, pero no se limitan a, los siguientes: el gesto del usuario principal 205 o el dispositivo 210; el movimiento del usuario principal 205 o el dispositivo 210; la orientación del usuario principal 205 o el dispositivo 210; y el comportamiento histórico en el tiempo, tal como la marcha, altura, movimiento, velocidad, gesto del usuario principal 205, o el rendimiento del usuario principal 205 a través de cualquier acto, gesto, movimiento o comportamiento en respuesta a un juego, desafío, estímulo o instrucción presentada en el dispositivo 210.

Los factores de ubicación pueden ser cualquiera de los siguientes, pero no se limitan a: la ubicación del usuario principal 205 o el dispositivo 210 en el registro frente a la autenticación; la ubicación del usuario principal 205 o el dispositivo 210 contra las restricciones de política del servidor predefinido 218; la proximidad del usuario principal 205 o el dispositivo 210 a otro usuario, dispositivo, sistema central o presentación; la proximidad del usuario principal 205 o el dispositivo 210 a la presentación 213; la ubicación o proximidad del usuario principal 205 o el dispositivo 210 contra una ubicación o proximidad anterior; la ubicación o proximidad absoluta del usuario principal 205 o el dispositivo 210 a cualquier punto conocido; el movimiento paralelo o contrario del usuario principal 205 o el dispositivo 210 contra una ubicación o proximidad.

Los factores de personalización pueden ser cualquiera de los siguientes, sin limitación: número de identificación personal personalizado (PIN) del usuario principal 205; desafío personalizado del usuario principal 205; secreto compartido del usuario principal 205 y el sistema central 215; desafíos o factores de terceros; fichas de hardware o factores de desafío; y factores impulsados por API, tal como la detección de la presencia de otros servicios, dispositivos, aplicaciones o datos.

Parte 3 - triangulación

La Figura 6 es un diagrama de flujo de bloques funcional de una modalidad del sistema y método de autenticación de contexto de seguridad móvil y muestra la triangulación entre el sistema central, la presentación, el dispositivo y el servidor. Como se muestra en la Figura 6, una modalidad del sistema y método de autenticación de contexto de seguridad móvil 301 incluye preferentemente: un usuario principal 205; un dispositivo 210; una presentación 213; un sistema central 215; un servidor 218; una aplicación 220; un canal de usuario 222; un canal del sistema central 224; y un canal inteligente 226. Preferentemente, la triangulación entre el sistema central 215, la presentación 213, el dispositivo 210 y el servidor 218 se mide en términos de línea de visión/sonido/sensación física. Esto puede ocurrir a través de la aplicación 220 en el dispositivo 210, el servidor 218, y los datos de ubicación digital tales como el GPS y el mapeo Geo-IP. Por ejemplo, el sistema central 215 puede proporcionar sus datos de ubicación digital a través del mapeo Geo-IP al proporcionar su dirección IP. De manera similar, el dispositivo 210 puede proporcionar además sus datos de ubicación digital a través de sus datos de GPS. Aunque la Figura 6 muestra la triangulación entre el canal de usuario 222; el canal del sistema central 224; y el canal inteligente 226, debe entenderse que pueden usarse múltiples canales sin apartarse del alcance de la invención.

Modalidades

En una amplia modalidad de la invención, se aplica como una capa de seguridad de autenticación por encima del nombre de usuario y contraseña, el inicio de sesión único o las implementaciones de inicio de sesión social como un enfoque de múltiples factores o defensa en profundidad para establecer la confianza, la autenticidad y el contexto de los miembros de un sitio web, aplicación, red, hardware de ordenador, software de ordenador o sesión de juegos de ordenador.

En otra modalidad, la invención podría usarse de forma independiente como un único medio para identificar y autenticar a un usuario o dispositivo frente a un servidor, sitio web o aplicación con un único escaneo y verificación de contexto triangulada.

Otra modalidad implica la aplicación de esta invención para forzar la autenticación para usuarios que acceden a ubicaciones físicas protegidas por entrada bloqueada, capaces de interactuar con un dispositivo informático electrónico móvil a través de la línea de sonido, visión, sensación, NFC y la entrada de datos textuales o el comando biométrico, tales como una puerta, ventana, vehículo o bóveda.

Otra modalidad implica establecer la verificación de contexto de autenticación para confirmar un pago, envío de formulario, acceso, modificación, interacción o ejecución de un proceso dentro de un programa, sitio web, aplicación, servidor, red o sesión donde el inicio de sesión/identidad no es el objetivo, sino la verificación en el proceso, el privilegio o la autorización de una acción por parte de un usuario o dispositivo previamente identificado y/o autenticado.

Otra modalidad implica la implementación de la invención en un entorno de medios (dispositivo decodificador, televisión, pantalla, cine, audio al aire libre, transmisión, evento en vivo, consola de juegos) donde el móvil y la pantalla interactúan para autenticar el contexto del usuario/dispositivo/ubicación para permitir el acceso, la interacción o el privilegio de vincularse con los medios, el juego o el contenido. Un ejemplo sería una habitación de hotel o una tienda con un DVR decodificador o capacidad de transmisión, cuyo acceso se autoriza a través de la autenticación mediante la invención.

Aún otra modalidad implica la aplicación de la invención con papel o materiales impresos para la autentificación en tiempo real y el procesamiento de pagos, comprobante de recibo o acuse de recibo, verificación de asistencia, acceso o permiso para entrar o vincularse con el contenido, la ubicación o los activos simbolizados por el material impreso. Los usuarios escanean el material y se autentican en el contexto de la ubicación, el dispositivo, el usuario, la sesión y otros factores.

Otra modalidad implica el uso de múltiples aplicaciones simultáneas de la invención de autenticación para coautenticar contextos que se superponen para proporcionar acceso mutuo a un activo común mediante múltiples usuarios, dispositivos o ubicaciones.

Otra modalidad implica utilizar la tecnología de la invención para proporcionar control de autenticación sobre medios sociales, contenido y conexiones, además de los mecanismos de seguridad nativos de las redes sociales, para proporcionar un control de usuario granular y de tiempo extendido sobre el acceso de contexto de pares autenticados, la descarga y la vinculación con ese contenido o conexiones.

Aunque la descripción escrita anterior de la invención permite a un experto en la técnica hacer y usar lo que actualmente se considera el mejor modo de la misma, los expertos en la técnica entenderán y apreciarán la existencia de variaciones, combinaciones y equivalentes de la modalidad, método y ejemplos específicos en la presente descripción. Por lo tanto, la invención no debería limitarse por la modalidad, el método y los ejemplos descritos anteriormente, sino por todas las modalidades y métodos dentro del alcance de la invención como se reivindica.

La descripción anterior de la modalidad preferida de la invención se ha presentado para fines ilustrativos y descriptivos. Aunque se describen múltiples modalidades, aún otras modalidades de la presente invención serán evidentes para los expertos en la técnica a partir de la descripción detallada anterior, que muestra y describe modalidades ilustrativas de la

invención. Como se comprenderá, la invención es capaz de modificaciones en varios aspectos obvios, todo ello sin apartarse del alcance de la presente invención. En consecuencia, la descripción detallada debe considerarse de naturaleza ilustrativa y no restrictiva. Además, aunque no se menciona explícitamente, una o más modalidades de la invención pueden llevarse a la práctica en combinación o juntas entre sí. Además, la referencia o la no referencia a una modalidad particular de la invención no deberá interpretarse como que limita el alcance de la invención. Se pretende que el alcance de la invención no se limite por esta descripción detallada, sino por las reivindicaciones y los equivalentes a las reivindicaciones que se adjuntan a esta presente descripción.

Excepto como se indica inmediatamente arriba, nada de lo que se ha indicado o ilustrado pretende o debe interpretarse que provoca una dedicación de cualquier componente, etapa, característica, objetivo, beneficio, ventaja o equivalente al público, independientemente de si se menciona o no en las reivindicaciones.

Reivindicaciones

1. Un método basado en ordenador para autenticar a un usuario a través de una red, las etapas que comprenden:
proporcionar un sistema central, un servidor, una presentación y un dispositivo;
en donde dicho dispositivo incluye una o más aplicaciones;
en donde dicho servidor incluye un algoritmo de perfil;
solicitar un acceso a dicho sistema central mediante un usuario principal en dicha presentación a través de un canal de usuario;
solicitar que dicho servidor realice una decisión de verificación de contexto mediante dicho sistema central a través de un canal del sistema central;
crear dos o más objetos de plantilla mediante dicho algoritmo de perfil de dicho servidor;
en donde dichos dos o más objetos de plantilla son una primera plantilla y una segunda plantilla; enviar un objeto a dicho sistema central a través de dicho canal del sistema central mediante dicho servidor;
presentar dicho objeto a dicho dispositivo en dicha presentación y a través de dicho canal de usuario mediante dicho sistema central;
procesar dicha primera plantilla mediante dicho servidor;
en donde dicha etapa de procesamiento de dicha primera plantilla se basa en uno o más factores contextuales;
llenar dicha primera plantilla mediante dicho servidor;
crear y almacenar una primera firma mediante dicho servidor;
en donde dicha etapa de creación de dicha primera firma se basa en dicha etapa de procesamiento de dicha primera plantilla;
consumir dicho objeto mediante dicho usuario principal en dicho dispositivo a través de dicha una o más aplicaciones;
solicitar dicha segunda plantilla en dicho servidor a través de un canal inteligente mediante dicha una o más aplicaciones;
enviar dicha segunda plantilla a dicha una o más aplicaciones en dicho dispositivo a través de dicho canal inteligente mediante dicho servidor;
procesar dicha segunda plantilla mediante dicha una o más aplicaciones;
llenar dicha segunda plantilla mediante dicha una o más aplicaciones; crear y almacenar una segunda firma mediante dicha una o más aplicaciones; en donde dicha etapa de creación de dicha segunda firma se basa en dicha segunda plantilla; y
realizar dicha decisión de verificación de contexto cuando se compara dicha primera firma y dicha segunda firma a través de dicho canal inteligente.

2. El método basado en ordenador de acuerdo con la reivindicación 1, en donde las etapas comprenden, además:

proporcionar uno o más factores externos adicionales a dicho dispositivo mediante dicho sistema central a través de dicho canal fuera de banda.

3. El método basado en ordenador de acuerdo con la reivindicación 1 o la reivindicación 2, en donde las etapas comprenden, además:

borrar dicho uno o más factores contextuales mediante dicho servidor.

4. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicha etapa de procesamiento de dicha segunda plantilla se realiza en base a uno o más factores contextuales.

5. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicha etapa de creación y almacenamiento de dicha primera firma se basa en dicha etapa de consumo de dicho objeto.

6. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones 1 a la 4, en donde dicha etapa de creación y almacenamiento de dicha primera firma se basa en dicha etapa de procesamiento de dicha segunda plantilla.

7. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, las etapas que comprenden, además:

ingresar uno o más datos fuera de banda en dicha una o más aplicaciones;
en donde dicho uno o más datos fuera de banda se transmiten a través de dicho canal fuera de banda.

8. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicha etapa de comparación de dicha primera firma y dicha segunda firma se realiza mediante dicho servidor.

9. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones 1 a la 7, en donde dicha etapa de comparación de dicha primera firma y dicha segunda firma se realiza mediante dicha una o más aplicaciones.

10. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, las etapas que comprenden, además:

autenticar dicho dispositivo cuando dicha primera firma es esencialmente idéntica a dicha segunda firma.

11. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicha etapa de creación y almacenamiento de dicha primera firma se basa en dicha etapa de consumo de dicho objeto.

12. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicha etapa de procesamiento de dicha primera plantilla se basa en uno o más factores contextuales.

13. El método basado en ordenador de acuerdo con la reivindicación 12, las etapas que comprenden además eliminar dicho uno o más factores contextuales mediante dicho servidor.

14. El método basado en ordenador de acuerdo con cualquiera de las reivindicaciones anteriores, en donde dicho rendimiento de dicha decisión de verificación de contexto cuando se compara dicha primera firma y dicha segunda firma a través de dicho canal inteligente es mediante dicho servidor y dicha una o más aplicaciones.

101

U = usuario	H = sistema central	S = servicio, servidor	C = canal
N = sesión	P = presentación	T = plantilla	F = factor
X = decisión	L = ubicación	B = comportamiento	O = objeto
R = registro	D = dispositivo	A = aplicación	Y = algoritmo de perfil

U1 = usuario principal	T0 = plantilla de servicio	U1 = ubicación del usuario
H1 = sistema central principal	T1 = plantilla de usuario/dispositivo	PL = ubicación de la presentación
N1 = sesión principal	FX = todos/cualquier factor	HL = ubicación del sistema central
C1 = canal de usuario	FD = factores del dispositivo	DL = ubicación del dispositivo
C2 = canal del sistema central	FP = factores personales	X0 = firma del servidor
C3 = canal inteligente	FL = factor de ubicación	X1 = firma del dispositivo/usuario
C4 = canal fuera de banda	FB = factor de comportamiento	01 = objeto de enlace
D1 = dispositivo original	FC = factor de personalización	R0 = primer registro
DN = dispositivo adicional	F0 = factor fuera de banda (OOB)	RN = registro posterior/nuevo registro

Cp = pin personalizado	Bg = gesto de comportamiento	Lo = ubicación original
Cc = desafío personalizado	Bo = orientación de comportamiento	Lp = ubicación de proximidad
Cf = tercera parte personalizada	Bm = movimiento de comportamiento	Lr = ubicación de registro
Co = fuera de banda personalizado	Bh = historial de comportamiento	Lg = ubicación de cerca geográfica
SSO = inicio de sesión único	Bc = personalización de comportamiento	La = ubicación asociativa
AX = el contexto	NFC = comunicación de campo cercano	Lh = historial de ubicación

Figura 1

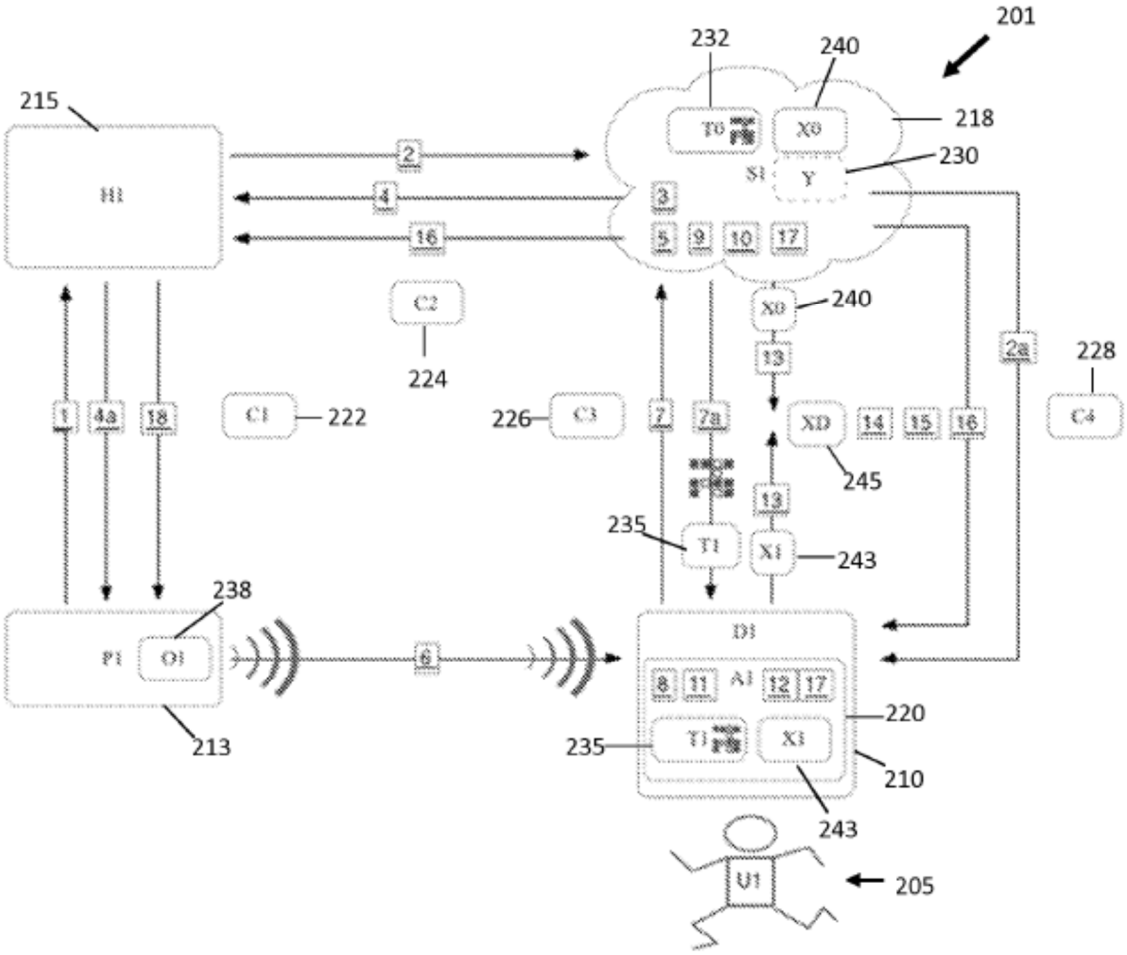
201
232
240
215
218
230
H1
T0
X0
S1
Y
2
4
16
3
5
9
10
17
C2
224
X0
240
13
2a
228
1
4a
18
C1
222
226
C3
7
7a
XD
14
15
16
C4
245
13
235
T1
X1
243
238
P1
O1
6
D1
8
11
A1
12
17
220
T1
X1
235
210
213
243
U1
205

Figura 2

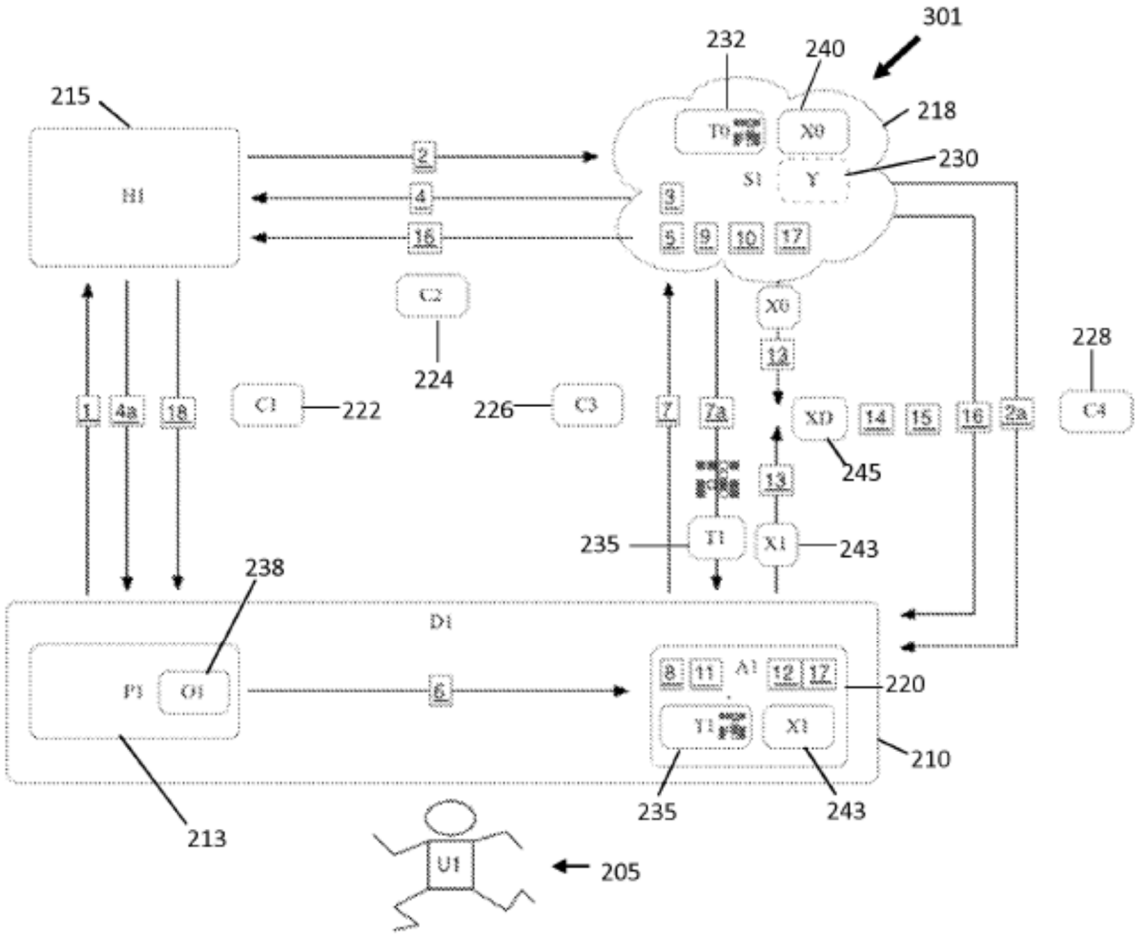
301
232
240
215
218
230
228
H1
T0
X0
S1
Y
2
4
16
3
5
9
10
17
C2
224
X0
12
1
4a
18
C1
222
226
C3
7
7a
XD
14
15
16
2a
C4
245
13
235
T1
X1
243
238
D1
P1
G1
6
8
11
A1
12
17
220
T1
X1
210
213
235
243
U1
205

Figura 3

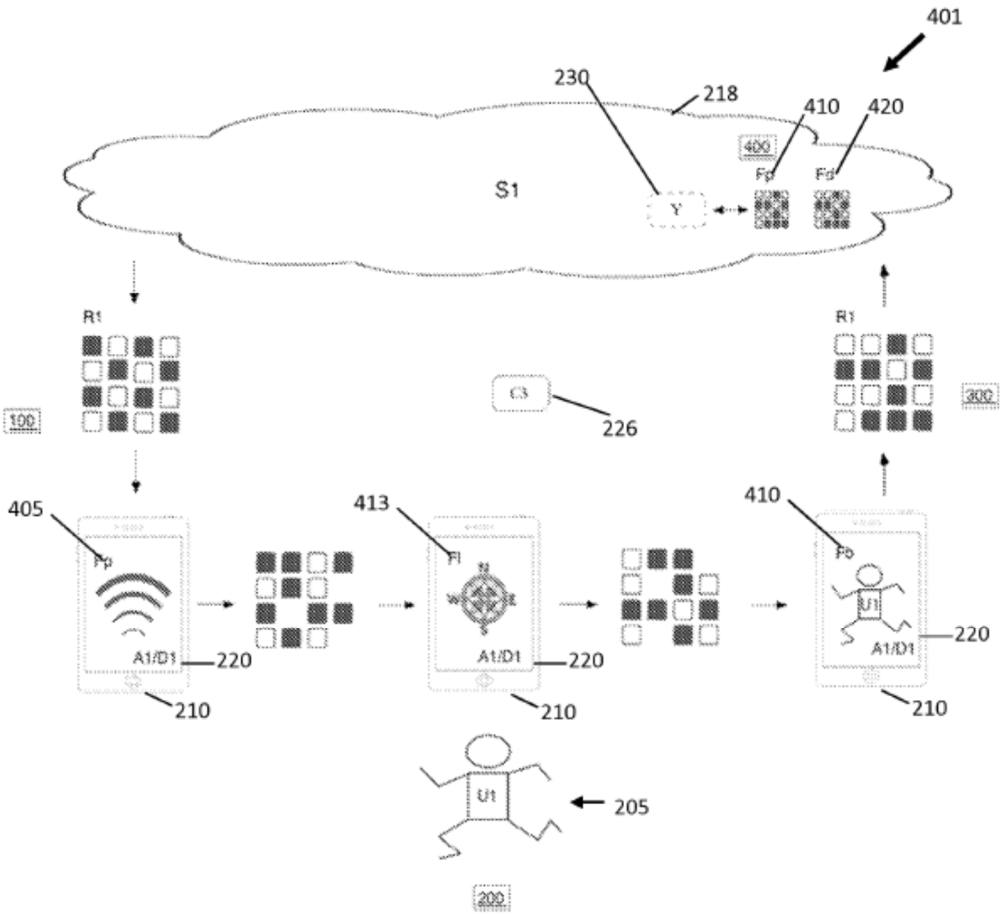
401
230
218
410
420
400
S1
Y
Fd
Fd
R1
100
C3
226
R1
300
405
Fp
413
Fl
410
Fb
U1
A1/D1
220
210
A1/D1
220
210
A1/D1
220
210
U1
205
200

Figura 4

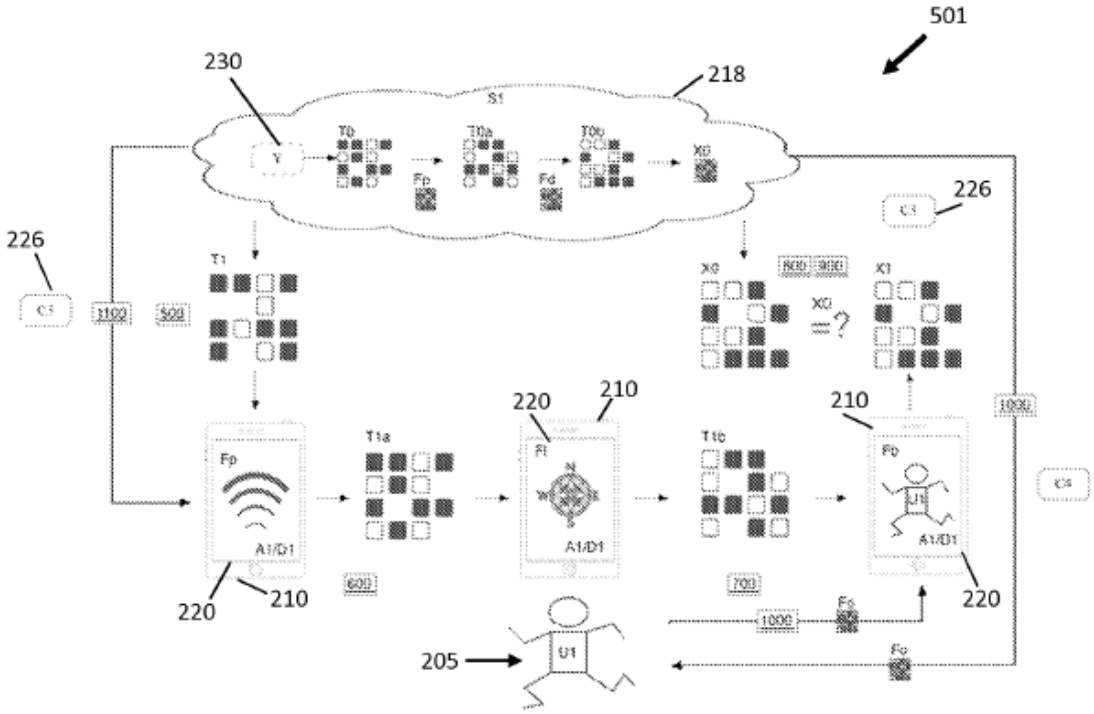
501
230
218
S1
T0
T0a
T0b
Fp
Fd
X0
226
C1
226
C1
T1
1102
502
X0
X0'
X1
220
210
Fp
A1/D1
T1a
Fi
A1/D1
T1b
210
Fb
A1/D1
220
C1
600
700
1000
Fg
Fg
205
U1
220
210

Figura 5

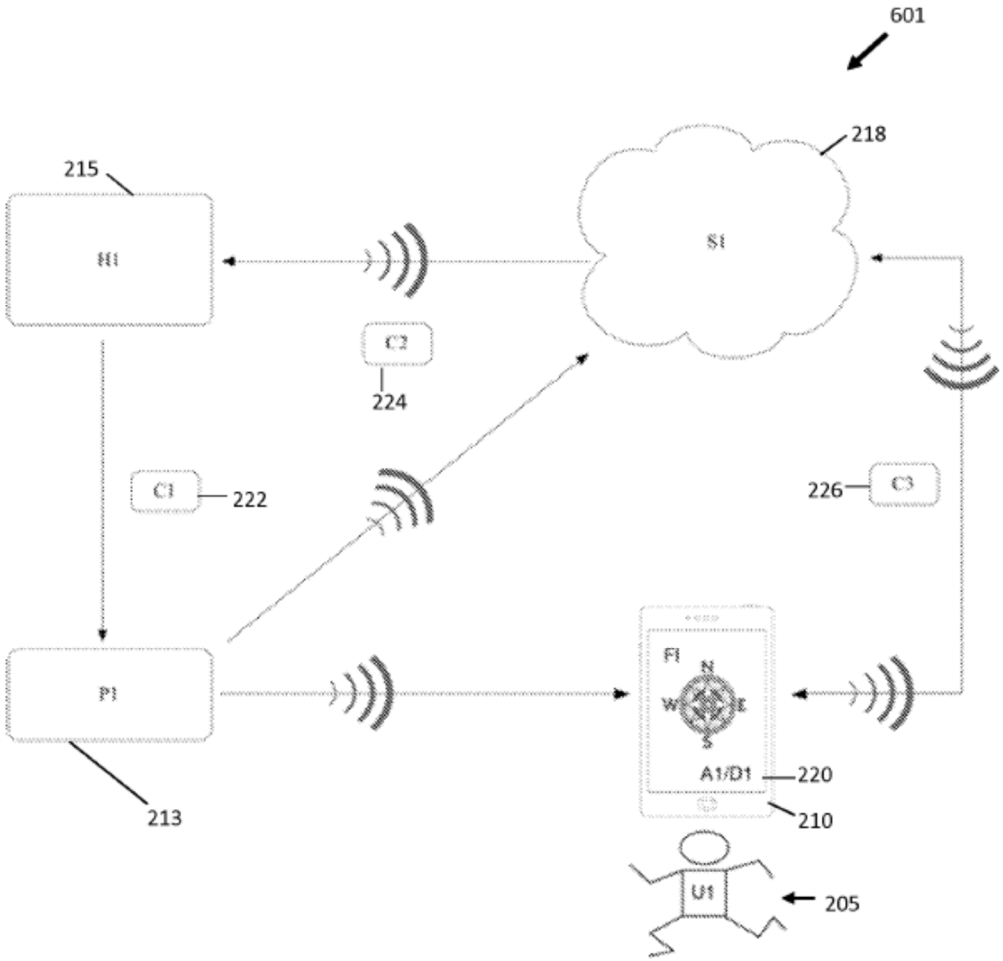
601
218
215
H1
S1
C2
224
C1
222
226
C3
P1
F1
N
W
E
S
A1/D1
220
210
213
U1
205

Figura 6