Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Autenticación de Múltiples factores (MFA)

Autor: Ing. Valentino Mantovani
Tutor: Dr. Juan Pedro Hecht

Año 2019
Cohorte 2018

1 Declaración Jurada de Origen de los Contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firma: [FIRMADO]

Nombres y Apellidos: Valentino Mantovani Cicilin

DNI: 34.950.983

2 Resumen

La autenticación de usuarios a los sistemas de información es uno de los puntos más delicados de los mismos, ya que una vez dentro (dependiendo de los privilegios) tenemos accesos a recursos que tal vez no deberíamos tener.

El uso de múltiples factores de autenticación es una de las soluciones a esta problemática, que se viene utilizando cada vez más para protegernos de diferentes ataques informáticos.

Está basado en la premisa de que un tercero no autorizado probablemente no pueda ser capaz de suministrar los factores requeridos para el acceso. Si en un intento de autenticación al menos uno de los componentes falta o se suministra incorrectamente, la identidad del usuario no se valida y no puede acceder a los recursos.

A los factores de autenticación los clasificaremos en:

- Algún objeto físico en posesión del usuario, como una memoria USB con un identificador único, una tarjeta de crédito, una llave, etc.
- Algún secreto conocido por el usuario, como una contraseña, un pin, una respuesta a una pregunta, etc.
- Alguna característica biométrica propia del usuario, como una huella dactilar, iris, voz, velocidad de escritura, patrón en los intervalos de pulsación de teclas, etc.

3 Tabla de contenido

4 Nómina de abreviaturas

2FA	Two Factor Authentication
2SV	Two Step Verification
BLE	Bluetooth Low Energy
CTAP	Client to Authenticator Protocols
FAR	False Acceptance Rate
FER	Failure-to-enroll Rate
CER	Cross-over Error Rate
FIPS	Federal Information Processing Standard
EER	Equal Error Rate
FRR	False Rejection Rate
HID	Human Interface Device
HOTP	HMAC-based One-time Password Algorithm
ISP	Internet Service Provider
IT	Information Technology
MFA	Multi-factor Authentication
NFC	Near Field Comunication
OTP	One Time Password
OWASP	Open Web Application Security Project
SFA	Single Factor Authentication
SMS	Short Message Service
TOTP	Time-based One-time Password algorithm
TPM	Trusted Platform Module
UAF	Universal Authentication Framework
USF	Universal Second Factor
W3C	World Wide Web Consortium

5 Introducción

Las contraseñas son cada vez más inseguras, tener un sistema que valide transacciones o accesos a recursos a través de una contraseña es inseguro. Dependemos de la robustez del sistema de autenticación y su infraestructura, si un atacante logra vulnerar este mecanismo tendrá acceso a los recursos que queremos proteger.

Esto es debido a que las contraseñas son un secreto compartido y es la clave única que demuestra que quien la posea es quien dice ser, autorizando a un sistema la autenticación de usuarios o la ejecución de ciertas transacciones. [2]

No podemos seguir pidiéndoles a los usuarios que refuercen aún más sus contraseñas, que tiene que tener 12 caracteres, al menos una minúscula, al menos una mayúscula, exigimos caracteres especiales, al menos un número y que el mismo no sea escalonado, además que esa contraseña no tenga en su interior el usuario ni datos personales. Les obligamos a cambiaras cada 1 mes y que la nueva que ingresen no debe ser igual a ninguna de las 8 anteriores. ¡Qué difícil!

El usuario repite sus contraseñas, no es posible que tenga en su cabeza la contraseña de Netflix, Gmail, Spotify, sus hombanking y el WiFi de su casa. Entonces un día se registra en un sitio de entretenimiento para comprar sus entradas de cine y resulta que esa entidad tiene un sus servidores una versión de Apache desactualizada y vulnerable. ¡Listo! No tengo que usar fuerza bruta para poder acceder a los demás servicios a los cuales está suscripto.

Una encuesta reciente realizada por Keeper Security[1] demuestra que: más del 80% de las personas de entre 18 y 30 años reutilizan la misma contraseña en diferentes aplicaciones. Lo que es más alarmante es que el 29% de los encuestados también admitió compartir contraseñas con dos o más personas.

[1] Es la empresa dueña del producto Keeper, un software que gestiona contraseñas muy conocido en el mercado. Más información en https://keepersecurity.com/es_ES/.

Es necesario brindarle al usuario otros mecanismos de seguridad que lo protejan y que al mismo tiempo no sean tediosos de utilizar.

Cada vez más los sistemas de información son imprescindibles para el desarrollo y la operación las empresas, cada vez más se almacena información valiosa y delicada, y es por eso que cada vez más los sistemas de información son objetivos de ataques por parte de hackers de sobrero negro, que quieren obtener esa información valiosa, generar denegaciones de servicios, monitoreo entre otras cosas.

Es tan importante la autenticación de los usuarios que OWASP (Open Web Application Security Project)[2] lo ha puesto en su última publicación dentro del TOP 10 publicada en el 2017 como la vulnerabilidad número dos, denominada Pérdida de Autenticación.

Una de las soluciones a esta problemática, que se viene utilizando cada vez más para protegernos de diferentes ataques informáticos vinculados al robo de identidad como lo son el phishing, los ataques de fuerza bruta, el robo de identificadores de sesiones, entre otras, es el uso de múltiples factores de autenticación, cada vez más son las aplicaciones que están ofreciendo de manera opcional a sus usuarios el uso de esta tecnología. ¡Vamos a ver de qué se trata!

[2] Es un proyecto de código abierto gestionada por una fundación sin fines de lucro creada para generar conciencia mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. Es popular por la publicación de un documento conocido como OWASP TOP 10 que advierte sobre los 10 riesgos de seguridad más comunes en aplicaciones web [1].

6 Objetivos

El presente trabajo tiene por objetivo la investigación de las diferentes metodologías de autenticación múltiple centrándonos especialmente en las 2FA o autenticación de dos factores, entender su funcionamiento y como nos pueden ayudar a mejorar las infraestructuras de autenticación de los nuevos sistemas o de los ya existentes.

Se pretende analizar cada una de ellas incluyendo sus pros y contras, costos de implementación, dificultades para usuarios finales, niveles de protección, vulnerabilidades, etc.

También se busca saber que hay en el mercado sobre esta tecnología y que tan difícil es implementarla dentro de una plataforma de software.

Hoy en día la mayoría de los sistemas de autenticación están configurados para soportar un solo factor de autenticación o factor de autenticación simple (SFA) lo cual es muy inseguro, es por eso que es también objeto de este trabajo generar conciencia sobre la importancia que tienen los mecanismos de autenticación múltiple.

7 Alcance

El alcance del trabajo es investigar las metodologías de autenticación múltiple, poder compararlas y sacar conclusiones sobre cada una de ellas.

También es de alcance de este trabajo el análisis de la implementación de autenticación de dos factores en aplicaciones web utilizando los protocolos creados por la FIDO (Fast IDentity Online) Alliance[3] que son UAF (Universal Authentication Framework) y U2F (Universal Second Factor), mas puntualmente, resumiendo en el reciente protocolo certificado por la W3C, el WebAuthn.

[3] La Alianza FIDO es un consorcio de la industria lanzado en febrero de 2013 para abordar la falta de interoperabilidad entre los dispositivos de autenticación fuerte y los problemas que enfrentan los usuarios al crear y recordar múltiples nombres de usuario y contraseñas. Nok Nok Labs , PayPal y Lenovo estuvieron entre los fundadores.

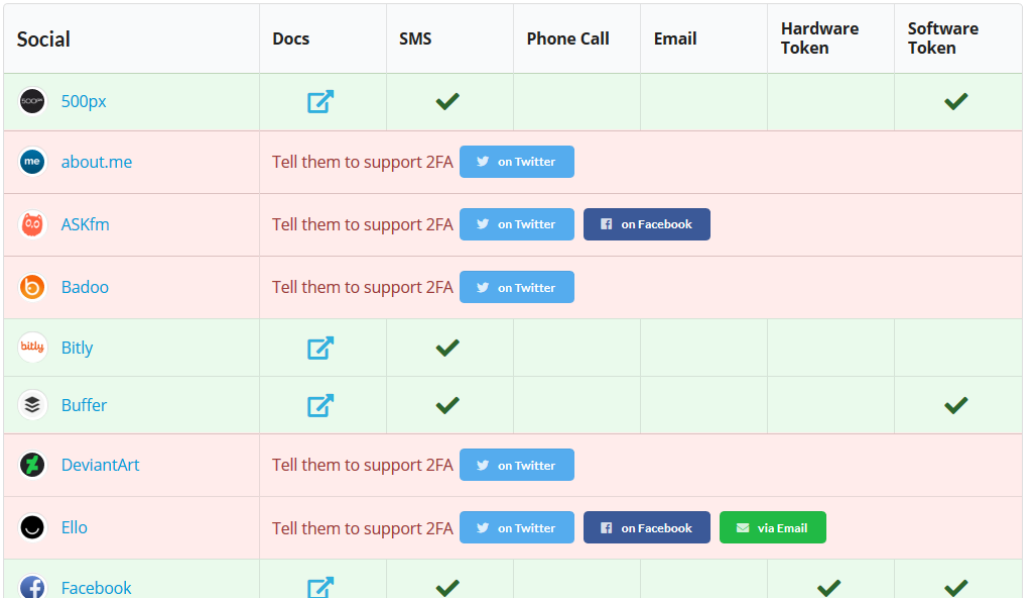
8 Metodologías de autenticación múltiple

Antes de comenzar, es necesario dejar en claro ciertas palabras que utilizaremos durante este trabajo. El PROBADOR es la entidad que quiere tener acceso a los recursos, es aquel que debe pasar por el VERIFICADOR, que es quien verifica la identidad y autoriza o no al probador a obtener estos recursos solicitados o bien aceptar la transacción requerida.

Primero debemos entender de manera clara el significado de “autenticación de múltiples factores” o MFA, que si bien las mismas palabras hablan por ellas, no estaría mal dejar algunos conceptos claros.

La autenticación de múltiples factores se refiere a realizar dos o más pruebas diferentes a un usuario para comprobar que es quien dice ser, con el objetivo de agregar una capa más de seguridad al verificador. Estas pruebas pueden ser diversas, como una contraseña, que posea una clave secundaria rotativa, un certificado digital instalado en el equipo, un token, etc. hablaremos más adelante sobre cada uno de ellos. [2]

Actualmente es muy común (y cada vez más) ver metodologías de autenticación de dos factores o 2FA, al menos opcionalmente para aquellos usuarios que quieran reforzar la autenticación de sus cuentas. Compañías como MercadoLibre, Google para el ingreso a Gmail, Apple para ingresar iCloud, Facebook y muchas entidades bancarias ya lo implementaron. La pagina web https://twofactorauth.org muestra todas aquellas compañías que implementaron ya esta metodología y se puede ver que cada día hay más que se involucran.



Social	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
500px	↗	✓				✓
about.me	Tell them to support 2FA on Twitter					
ASKfm	Tell them to support 2FA on Twitter on Facebook					
Badoo	Tell them to support 2FA on Twitter					
Bitly	↗	✓				
Buffer	↗	✓				✓
DeviantArt	Tell them to support 2FA on Twitter					
Ello	Tell them to support 2FA on Twitter on Facebook via Email					
Facebook	↗	✓			✓	✓

Ilustración 1: sitio web https://twofactorauth.org muestra las redes sociales involucradas con 2FA

Se puede ver también cuando vamos al cajero automático a retirar dinero, requerimos de dos factores para poder completar la operación: una tarjeta de debito (algo que tenemos) y un pin o contraseña (algo que sabemos).

También es necesario saber para qué sirven o cual es el objetivo de estos sistemas de autenticación de múltiples factores. Esta tecnológica es utilizada para poder verificar de manera fehaciente la identidad de una persona, que quiera realizar alguna transacción o acceder a un sistema de información, a un edificio, una caja fuerte, un arma de guerra, en fin, un bien preciado y que no caiga en manos de un tercero no autorizado, entonces, sí al menos uno de estos factores suministrados no se puede satisfacer, el verificador niega la transacción al probador. [2]

9 Factores de autenticación

Los MFA utilizan pruebas para poder validar correctamente la transacción solicitada, estas pruebas las agrupamos en factores de distintos tipos y los clasificamos para poder estudiarlos mejor y para poder armar una definición más clara de las premisas o requerimientos que debe tener un verificador para poder realizar un autenticado de múltiples factores. [3][2]

Comenzaremos realizando una pequeña clasificación para entender cómo se dividen los factores para autenticar:

- Basados en algo que conozco. Por ejemplo: un ping, una contraseña, fechas de nacimiento, el nombre de mi primer mascota, etc.
- Basados en algo que poseo. Por ejemplo: una tarjeta de crédito, un token, una tarjeta de coordenadas, un certificado digital, etc.
- Basados en alguna característica física o acto involuntario del probador. Por ejemplo: una huella, patrones de escritura, de la voz u oculares, etc.

9.1 Factores de conocimiento

Están basados en algo que conozco, los factores de conocimiento son la forma más común de autenticación. El usuario necesita demostrar que conoce un secreto para poder autenticarse, como por ejemplo un ping, una contraseña, fechas de nacimiento, el nombre de su primer mascota, etc. [2]

Muchos sistemas de autenticación de múltiples factores confían en las contraseñas como uno de los factores de autenticación. Estos sistemas pueden precisar que se utilicen contraseñas más largas de múltiples palabras y otros una clave más corta.

Se espera que estas contraseñas sean memorizadas y no compartidas con nadie y menos anotadas en post-it en el monitor de una computadora personal. Es de esperar que los sistemas de autenticación no

utilicen las preguntas de seguridad[4] como método de verificación es un ejemplo débil en seguridad, puesto que suelen referirse a información conocida por el entorno del usuario, de dominio público o que se pueden averiguar fácilmente realizando una simple investigación.

9.2 Factores físicos

Basados en algo que poseo, los factores físicos han estado en uso desde que se tiene conocimiento, el ejemplo más básico es el de la llave de una cerradura. El principio básico es que la llave simboliza un secreto que se comparte con la cerradura, y el mismo principio subyace en los sistemas de computadoras que utilizan factores físicos de autenticación. Una tarjeta de crédito, un token, una tarjeta de coordenadas, un certificado digital son ejemplos de estos factores. [2]

Podemos distinguir entre dos tipos de tokens:

9.2.1 Token sin conexión

Los tókens sin conexión son generados sin que el dispositivo tenga conexión a la computadora en la que el usuario se quiere autenticar. Normalmente utilizan una pantalla integrada para mostrar la información de autenticación que genera, y que luego el usuario debe introducir manualmente en la computadora. Estos tokens generan una contraseña de un solo uso ó OTP que es válida solo para el proceso de verificación en una ventana de tiempo determinado.

Que se denominen tokens sin conexión no significa que no necesitan estar contactados a internet, existen múltiples implementaciones que van desde el uso de complejos algoritmos matemáticos, uso de tablas desafío-respuesta, al uso de sincronizaciones de tiempo utilizando el protocolo NTP.

[4] Las preguntas de seguridad son utilizadas para validar el ingreso de un usuario en algunos sistemas. Al momento de la creación de la cuenta nos realizan preguntas como *¿Cuál es el nombre de tu primera mascota?* Luego se utiliza la respuesta para validar el ingreso ó alguna acción determinada.

9.2.2 Token conectados

Los tókens conectados son dispositivos que están físicamente conectados a la computadora con la que se van a utilizar, y por tanto transmiten información automáticamente. Existen distintos tipos, como por ejemplo lectores de tarjetas, etiquetas inalámbricas y tókens USB como las famosas llaves Yubikey[5] o las Titan de Google.

9.3 Factores inherentes

Son factores que están asociados al usuario, y generalmente son métodos biométricos, como los lectores de huellas, de retina o reconocimiento de voz. Estos factores se están utilizando cada vez más ya que además de ser seguros los dispositivos móviles de última generación han mejorado la tecnología de hardware y lo traen consigo. [2]

No quiero dejar de lado a aquellos factores inherentes que realizan la verificación sin el uso de sensores, sino que utilizan el reconocimiento de patrones, como el movimiento del mouse, dinámica de tecleo, que gracias a la inteligencia artificial son cada vez más eficientes generando menos casos de falsos positivos. Los veremos con más detalles más adelante.

9.4 Otros factores

Existen otros factores que son menos utilizados pero no por eso dejaremos de nombrarlos, como el tiempo o el factor de ubicación, que permite a través de una antena de GPS ó una dirección IP podríamos verificar la ubicación de un usuario y negarle el acceso si no se encuentra en ese lugar o por ejemplo, si esta dentro de una red de trabajo utilizar solo un PIN para ingresar los sistemas del trabajo y fuera de ella utilizar un factor adicional.

Es importante combinar estos tipos factores de autenticación, ya que si seleccionan de manera incorrecta el sistema de MFA sería inútil, de hecho

[5] Es un dispositivo de autenticación de hardware fabricado por Yubico que generan claves del tipo OTP y se hicieron muy populares por su bello diseño y practicidad para conectarse a varias plataformas conocidas. Se puede ver más información en https://www.yubico.com/.

por definición deberíamos tener al menos dos factores involucrados, de lo contrario dejaría de ser un MFA.

10 Autenticación de dos factores

Tal vez se pregunten porque elegí centrarme y acotar el estudio de los MFA, solo a los sistemas de autenticación de dos factores, y esto es porque son los más populares y porque ya nos alcanza para poder entender cómo funcionan los MFA, ya que para los demás solo es necesario agregar más factores. Uno de los problemas que ya se están sabiendo cómo resolver de los sistemas de tres o más factores, es que resulta demasiado tedioso para el probador realizar tantas validaciones; en seguridad informática debemos tratar de conseguir un equilibrio entre lo amigable y lo seguro, ya que podemos correr el riesgo de tener un sistema muy seguro pero que nadie lo quiera utilizar.

Actualmente existen empresas que brindan soluciones de tres factores de autenticación pero que permiten que el probador pueda validar dos de las tres pruebas. Esto muchas veces hace que el sistema sea más inseguro que uno de dos factores ya que existe una variable más que puede ser comprometida.

Los requerimientos de seguridad de la industria y las regulaciones están en constante cambio para poder dar respuesta a las amenazas emergentes es por eso que tal vez el futuro se empiecen a ver verificadores con más de dos factores de autenticación, de hecho existen cajeros automáticos que validan al probador biométricamente, a través de sus huellas dactilares, no sería difícil pensar que este último factor sea requerido solo para operaciones más importantes como extracciones o transferencias de dinero.

10.1 Autenticación de dos pasos

Muchas veces se suele confundir a la 2FA con 2SV ó la autenticación de dos pasos ya que parecen ser lo mismo pero no lo son.

Se dice que la autenticación de dos pasos es una expansión de la autenticación simple y es muy utilizada en los inicios de sesión de algunos sitios web. Veamos cuales son los pasos que debe seguir un sistema 2SV:

1- El probador ingresa usuario y contraseña.
2- Se envía un código OTP o de un solo uso mediante un email, SMS o llamada telefónica generalmente a un dispositivo móvil.
3- El probador ingresa el código recibido para completar el acceso a la cuenta. Este código tiene una ventana de tiempo en el cual puede funcionar, luego quedara inutilizado.

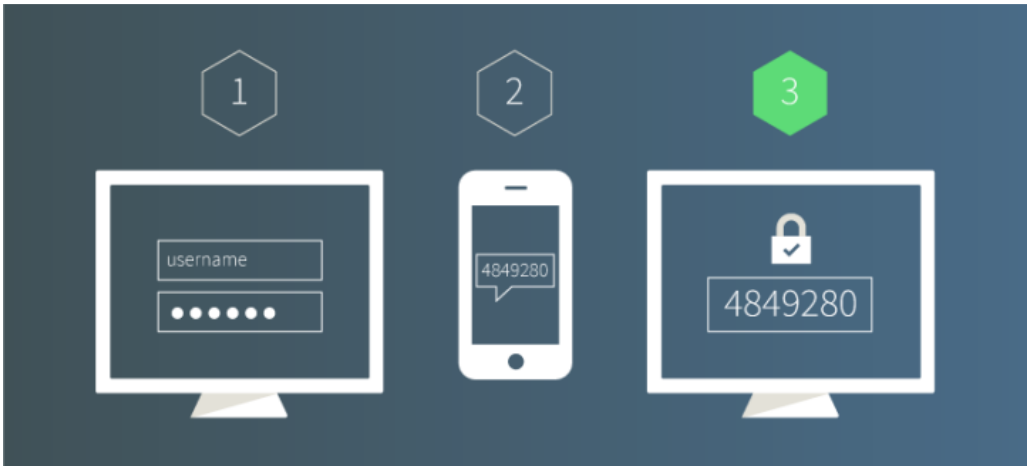


Ilustración 2: pasos para iniciar sesión utilizando los mecanismos de autenticación de dos pasos.

Si bien el dispositivo a donde llega el código OTP puede parecer un factor físico ("algo que poseo"), no lo es desde el punto de vista de la seguridad informática, que sigue siendo un factor de conocimiento ("algo que conozco"). Esto se debe a que la clave para la autenticación no es el dispositivo en sí, sino la información almacenada en el dispositivo que, en teoría, podría ser copiada por un atacante. Por lo tanto, al copiar tanto su contraseña memorizada como la configuración de OTP, un atacante podría suplantarlo sin robar nada físico.

La diferencia entre estos dos conceptos fue distinguida por varios expertos en seguridad informática pero no todos están de acuerdo, podemos ver en la siguiente imagen lo que nos dice Google cuando queremos activar la verificación de dos pasos, habla de los dos conceptos como si no existiera diferencia alguna.

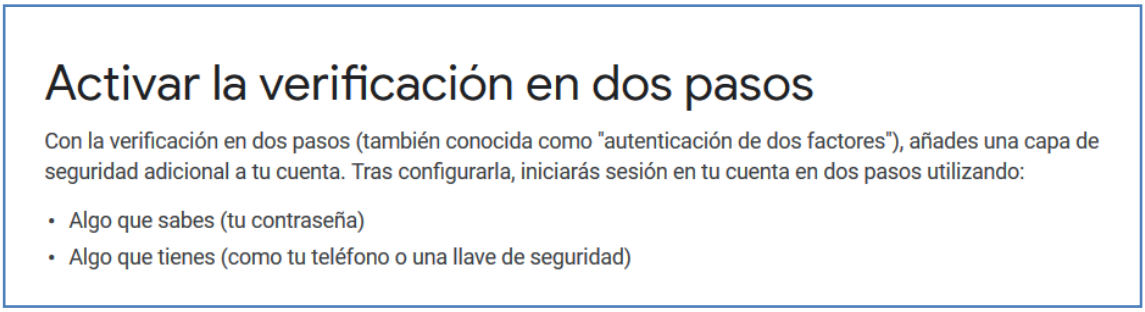


Ilustración 3: descripción de verificación de dos pasos de Google.

A efectos de este trabajo, diremos que existe una diferencia entre ambos conceptos, como antes ya mencionamos, distinguiendo a la 2FA por sobre la 2SV en cuanto a la seguridad como mecanismo de autenticación, sin embargo, incluiremos a las metodologías de 2SV dentro de los diferentes casos que nos presentan los MFA.

10.2 Segundos factores de autenticación

Listaremos a continuación los segundos factores de autenticación más comunes que son utilizados y que podemos encontrar en las aplicaciones más populares.

10.2.1 Códigos SMS

Se trata de un código OTP que es enviado a través de un mensaje SMS a un dispositivo celular del probador. Este código es generado por el verificador y tiene un tiempo de expiración. Es necesario que este código solo sea conocido por el probador y el verificador, lamentablemente este es uno de los segundos factores de autenticación más vulnerables como veremos con detalles más adelante.

10.2.2 Llamada telefónica

Similar al de los SMS, con la diferencia que se puede realizar a teléfonos fijos además de teléfonos celulares. En este caso existen dos variantes. Por un lado la que al atender un maquina te deletrea un OTP con la opción de volver a repetirlo y por otro lado la que nos pregunta si queremos aceptar o no el ingreso, por ejemplo, presione 1 (uno) si desea aceptar o 2 (dos) si desea denegar el acceso.

10.2.3 Notificaciones push

Este mecanismo es más seguro que los anteriores, depende sobre todo de la confianza del proveedor. Aquí no se generan códigos OTP, sino que debemos tener instalada una aplicación en nuestros celulares y la misma activara una notificación push que preguntara si aceptamos o no el ingreso a la cuenta.

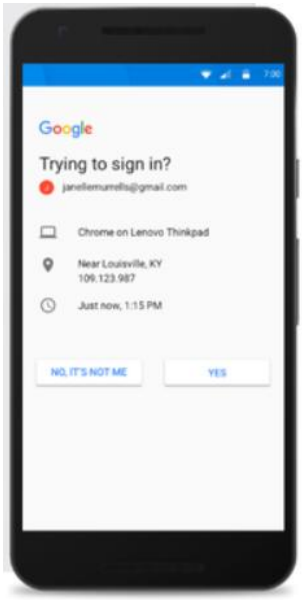
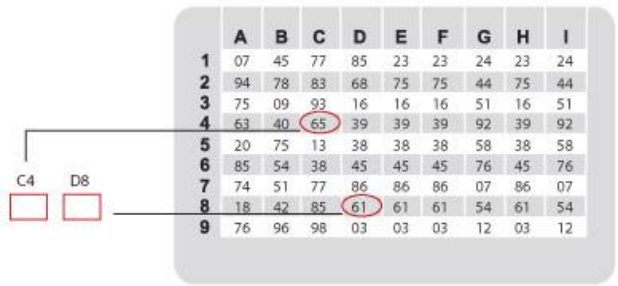


Ilustración 4: Google A2F

Este método es ofrecido por Google a sus usuarios como segundo factor de autenticación. Una vez configurado, cada vez que ingresemos nuestros usuario y contraseña de manera correcta en una PC no registrada, Google nos enviará una notificación push a nuestro celular donde figura: el navegador del cliente desde donde se están conectado, la dirección aproximada (obtenida a través de la ip publica brindada por el ISP) y el día y hora de la petición. Debajo nos muestra dos botones para que aceptemos o revoquemos el ingreso solicitado.

10.2.4 Tarjetas de coordenadas

La tarjeta de coordenadas es una tarjeta de plástico, del tamaño de una tarjeta de crédito, que contiene una matriz o serie de números (generalmente pares de datos) impresos, es decir, ordenados en filas y columnas. Las filas están tituladas con números ascendentes a partir del 1 y las columnas con letras ascendentes alfabéticamente comenzando desde la A. En algunos casos, el orden es inverso: en las filas se encuentran las letras por orden alfabético, y en las columnas los números. Para una tarjeta de 100 coordenadas se necesitan 10 filas (del 1 al



	A	B	C	D	E	F	G	H	I
1	07	45	77	85	23	23	24	23	24
2	94	78	83	68	75	75	44	75	44
3	75	09	93	16	16	16	51	16	51
4	63	40	65	39	39	39	92	39	92
5	20	75	13	38	38	38	58	38	58
6	85	54	38	45	45	45	76	45	76
7	74	51	77	86	86	86	07	86	07
8	18	42	85	61	61	61	54	61	54
9	76	96	98	03	03	03	12	03	12

Ilustración 5: tarjeta de 81 coordenadas.

10) y 10 columnas (de la A a la J). La primera celda se llamará A1 y la última J10. [2]

Es como un PIN dinámico, son usadas generalmente por entidades bancarias para validar operaciones como transferencias bancarias, depósitos de dinero o pago de algún servicio entre otras. El sistema para poder validar la operación pide al probador que ingrese dos de los números que figuran en la tarjeta, como por ejemplo, las que se ve en la imagen, las celdas C4 y D8.

10.2.5 Correo electrónico

El correo electrónico es otra forma de validar una transacción aunque no es utilizado generalmente para la autenticación. Si se puede ver que varias aplicaciones lo utilizan para validar un registro y validar la creación de cuenta.

Medium es una red social de los creadores de Twitter. Esta red social tiene la particularidad que solo es posible registrarse con una cuenta de Facebook o Google utilizando el protocolo OAuth2. Para autenticarse, esta red social también utiliza formas poco convencionales pero validas en términos de seguridad, permite hacerlo de dos maneras: por un lado utilizando OAuth2 al igual que en el registro y por el otro a través del correo electrónico registrado, manda un correo con un link válido solamente por 15 minutos luego de haber sido generado y que puede ser utilizado solo una vez.

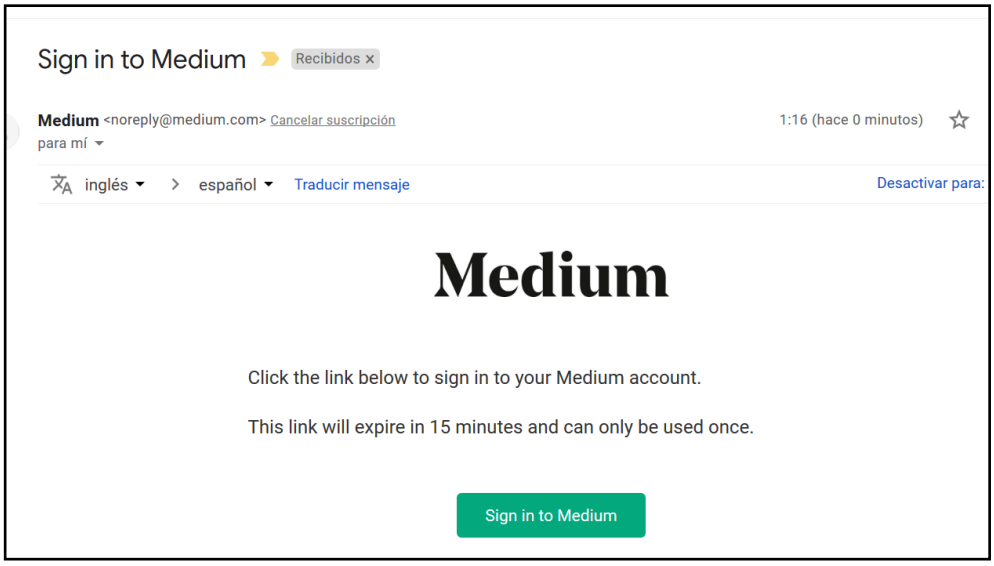


Ilustración 6: email donde muestra el link de autenticación para una cuenta de Medium.

10.2.6 Software Token

Ésta es la metodología más utilizada ya que hace un importante equilibrio entre costos y seguridad. Se trata de un sistema de generación de códigos OTP que fue configurado previamente a través del intercambio de una clave que es conocida por el sistema de generación de claves y el sistema de autenticación, existen dos maneras de generación de claves OTP:

- TOTP (contraseña de un solo uso basada en el tiempo): esta metodología utiliza la clave intercambiada en la configuración y la hora actual, redondeada en 30 segundos. Ambos componentes son los mismos para el generador y el sistema de autenticación, por lo que los códigos se generan de forma sincronizada.
- HOPT (contraseña de un solo uso basada en HMAC): en lugar de la hora actual, este algoritmo utiliza un contador que aumenta en 1 por cada código recién creado. El contador y la clave simétrica son las entradas a un algoritmo de hash usando HMAC (como por ejemplo el HMAC-SHA1) generando un token que se valida con el servidor que sigue los mismo pasos. Esta metodología no es tan utilizada ya que su uso complica la generación sincrónica de códigos por parte del generador y el sistema de autenticación, es decir, si por algún motivo

esta sincronización se pierde, los códigos ya no servirán, el sistema no autenticará y deberán sincronizarse nuevamente los sistemas. [2]

Generalmente podemos ver en el mercado aplicaciones para Smartphone que pueden ser utilizadas para el segundo factor, la gran mayoría de las aplicaciones utilizan el mismo algoritmo, por lo que se puede utilizar cualquiera para servicios que admitan autenticadores. Hay excepciones en donde ciertos servicios utilizan sus propias aplicaciones y no funcionan con los genéricos entre los cuales se encuentran los principales editores de videojuegos, como, por ejemplo, Blizzard Authenticator, Steam Mobile con Steam Guard incorporado, Wargaming Auth, algunos bancos incorporan esta funcionalidad en sus aplicaciones de homebanking generalmente para válidar ciertas transacciones como transferencias bancarias, inversiones, etc. Instituciones como Santander Rio, Banco Nación, Banco Galicia, entre otros, brindan este servicio.

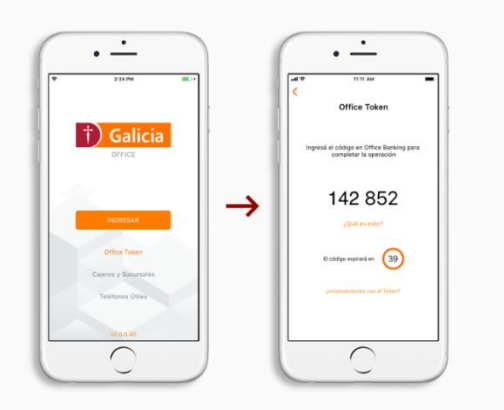


Ilustración 7: app generador de tokens de Banco Galicia

Todas las aplicaciones mencionadas anteriormente generan sus propios algoritmos de cifrado y son incompatibles con aplicaciones genéricas y servicios de terceros. Existen en el mercado varias aplicaciones que generan estos tokens, algunas con más funciones que otros. Esto se puede comprobar ingresando al distribuidor digital de aplicaciones móviles de algún dispositivo, sea Google Play para Android o App Store de Apple, entre los más recomendados se encuentran Google Authenticator, Duo Mobile, Microsoft Authenticator, Authy y Yandex. [5]

10.2.7 Hardware Token

Aquí volvemos a remarcar la diferencia entre los tokens con/sin conexión. Por un lado existen tokens físicos que al igual que los de software,

generan códigos de un solo uso para validar una transacción pero lo hacen a través de algún dispositivo físico.

Por otro lado aquellos tokens llamados llaves de autenticación, generalmente son dispositivos USB o con antenas de corto alcance como NFC, RFID o bluetooth. Durante la configuración de la llave, la misma genera una secuencia de 44 caracteres que está relacionada exclusivamente con el dominio del sitio en el cual el usuario está realizando la configuración. De esta manera logramos evitar ser víctimas de *phishing.* El funcionamiento es muy sencillo. El usuario ingresa sus datos de inicio de sesión y luego el navegador le solicitará que conecte la llave en el puerto USB de su computadora personal (o la apoye en el lector NFC de su Smartphone) para superar el desafío. [6]

Ilustración 8: iniciando sesión en Google con un hardware token.

La mayoría de estos tokens soportan el estándar U2F, que evoluciono en FIDO2 y luego en WebAuth[6], creado por FIDO Alliance, son los más populares, ya que son muy fáciles de ponernos en funcionamiento, además, recientemente (año 2019) la W3C ah declarado a WebAuth como un estándar web abierto oficial utilizando el mismo como API para autenticar usuarios con estos tokens. Actualmente es soportada por la mayoría de los navegadores como Microsoft Edge, Mozilla Firefox y Apple Safari que ya lo implementan desde el año 2018, como así también las plataformas más conocidas. Android es un ejemplo, que a partir de su versión 7.0 en adelante los usuarios de este sistema operativo de Google tienen la posibilidad de utilizar las claves de seguridad FIDO para el inicio de sesión de forma

[6] U2F, FIDO2 y WebAuth son estándares creados por la FIDO Allance. Veremos más adelante el detalle de cada uno de estos, para que funcionan y cómo se utilizan.

segura en páginas web y aplicaciones nativas o, mucho mejor, con el sensor de huellas dactilares integrado en el equipo. Hablaremos con más detalles de estos protocolos más adelante. [5][6]

Estos tokens también se utilizan para almacenar certificados digitales y de esta manera poder validar la identidad a través de una autoridad certificante. En la Argentina la secretaría de modernización monto una estructura para que el ciudadano pueda realizar trámites válidos jurídicamente al igual que un documento en papel firmado de puño y letra garantizando de esta manera que no pueda ser objeto de repudio a través de una firma digital, en la cual el gobierno es una certificadora raíz y entrega/revoca certificados a los solicitantes. Para poder obtenerlo es necesario simplemente llenar un formulario y disponer de un token FIPS 140-2[7] nivel 2 o superior. [7]

Actualmente son los segundos de factores de autenticación más seguros del mercado aunque los más costosos al mismo tiempo.

10.2.8 Biométricos

Este segundo factor de la categoría de los inherentes, es cada día más popular debido a la confiabilidad que ha tomado de acuerdo con el avance de la tecnología y a que los costos de estos dispositivos son cada vez más accesibles.

Es más fácil encontrarlos en los ingresos a edificios o áreas restringidas cómo salas de servidores, a veces incorporado para el control de asistencia (reconociendo la entrada y salida de un individuo) y otras para el control de acceso. Sin embargo, es cada vez es más común verlos también en computadoras portátiles y teléfonos celulares abriendo el espectro para el uso de otras aplicaciones.

[7] Es un estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. El nivel 1 requiere algoritmos probados externamente. El nivel 2 agrega requisitos para la evidencia de manipulación física y la autenticación basada en roles. Ademas de ciertos requisitos sobre el software donde se realiza la implementación. [7]

En el 2016 una encuesta realizada por VISA en Europa determinó que dos tercios de los europeos preferirían usar una autenticación biométrica para sus pagos o transacciones a través de Internet. Se trata de una proporción notable e indica las preferencias de la mayoría de usuarios de Internet[8].

Hablaremos con más detalles sobre esta tecnología en el próximo capítulo.

[8] Se puede ver más sobre este estudio en la siguiente web: https://www.finextra.com/newsarticle/29171/europeans-keen-to-secure-payments-with-biometrics

11 La autenticación biométrica

La autenticación biométrica es el proceso de verificar la identidad de un sujeto utilizando las características únicas de su cuerpo o a través de su comportamiento, para iniciar sesión en un servicio, una aplicación, un dispositivo o bien realizar alguna transacción. [8]

Este sistema cuenta de dos partes: el registro, donde una persona se de de alta en el sistema de autenticación utilizando una o más de sus características físicas y de conducta, que es procesada por un algoritmo numérico e introducida en una base de datos para utilizarla luego en la comparación de identidad, la segunda etapa. Esta etapa consiste en comparar los datos de la prueba realizada por la persona o probador con los almacenados, y si estos dos datos son casi idénticos, el dispositivo o verificador puede dar acceso o aprobar la transacción solicitada.

Es importante tener en cuenta que la coincidencia entre los dos conjuntos de datos tiene que ser casi idéntica, como mencionamos en el párrafo anterior, pero no exactamente idéntica. Esto se debe a que es casi imposible que dos datos biométricos coincidan al 100% debido a que por ejemplo en pruebas de huellas dactilares, se puede tener un dedo sudoroso o una pequeña cicatriz que cambia el patrón de impresión. [13][14]

En la mayoría de los dispositivos biométricos es posible configurar la sensibilidad a la hora de la comparación, mediando entre la usabilidad y la seguridad. El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (FAR), que mide aquellos casos en donde se verifica o identifica incorrectamente a una persona no autorizada, es también conocido como error de tipo II, una aceptación falsa generalmente se considera el más grave de los errores de seguridad biométrica, ya que brinda a los usuarios no autorizados acceso a sistemas que expresamente intentan mantenerlos fuera. La tasa de falso negativo (FRR) donde medimos exactamente lo contrario que en FAR, son aquellos casos donde no se autorizo a una persona que debería haber sido autorizada. Y la tasa de fallo de alistamiento (FER), que mide aquellos casos

de fracaso de la primera etapa, es decir del registro de los datos del sujeto al sistema biométrico, esto implica que tengamos problemas luego en la comparación de datos, es por eso que muchos sistemas piden por ejemplo que se ingrese más de una vez la huella en el momento del registro de la misma. [8][14]

Una de las medidas más comunes de los sistemas biométricos reales es la tasa de error igual (EER), un algoritmo del sistema que se usa para predeterminar los valores de umbral para su tasa de aceptación falsa y su tasa de rechazo falso. Cuando las tasas son iguales, el valor común se denomina tasa de error igual. Este indica que la proporción de aceptaciones falsas es igual a la proporción de rechazos falsos. Es inversamente proporcional a la precisión, es decir, cuanto menor sea el valor de la tasa de error igual, mayor será la precisión del sistema biométrico. La EER también es conocida como la tasa de error de cruce (CER).

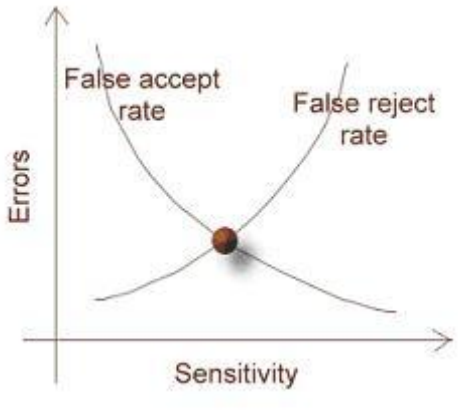


Ilustración 9: tasa de error igual.

Para que las características físicas y conductuales sean utilizadas como elementos de identificación deben cumplir con los siguientes requisitos mencionados por el Ing. MSc. Gerson Enrique Delgado Parra en su artículo Biometría: [9]

a) Universalidad: todas las personas tienen o presentan una característica.
b) Singularidad: dos personas cualesquiera son distinguibles una de la otra en base de sus características.
c) Estabilidad: la característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas.
d) Cuantificable: la característica tiene que ser mesurable cuantitativamente.

e) Aceptabilidad: el nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico.
f) Rendimiento: el nivel de exactitud requerido debe ser elevado para que la característica sea aceptable.
g) Usurpación: permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.

Existen muchos factores biométricos que pueden servir para la autenticación, veremos a continuación los más utilizados.

11.1 Huella dactilar

Es tal vez uno de los más populares es la huella dactilar, que es también uno de los más antiguos. En la actualidad la mayoría de los smartphones ya cuentan con uno de ellos para el desbloqueo de la pantalla, y el objetivo es utilizarlos también para esta causa.

Ilustración 10: desbloqueo de WhatsApp con huellas dactilares en Android.

Existen tres variedades de ellos: [16]

- **Ópticos**: toma una fotografía del dedo, identifica el patrón de impresión y luego lo compila en un código de identificación.
- **Capacitivos**: funciona midiendo las señales eléctricas enviadas desde el dedo al escáner. Las crestas de impresión, que tocan directamente el escáner, envían corriente eléctrica, mientras que los valles entre las crestas crean espacios de aire. Un escáner capacitivo mapea estos puntos de contacto y huecos de aire, lo que resulta en un patrón único.
- **Ultrasonido**: estos emiten ultrasonidos que se reflejan en el escáner y, similar a uno capacitivo, forman un mapa del dedo único para el individuo. No necesita el contacto directo, basta con colocar el dedo en el punto indicado para que los ultrasonidos

vayan directos a la yema, reboten y sean interpretados por un lector especialmente diseñado para ello. Son más precisos ya que son capaces de saltar obstáculos e interferencias para la identificación como el sudor, suciedad, temperatura, crema de manos, etc.

En Argentina ANSES puso en práctica el plan Mi Huella, una iniciativa que tuvo fecha límite de enrolamiento el pasado 30 de junio del 2019 y con el cual la institución se asegura la supervivencia o fe de vida del jubilado o pensionado. Otro ejemplo es el que realizo el Banco Santa Fe en la ciudad de Rosario, instaló el primer cajero automático de la provincia con identificación de huellas dactilares, para que los usuarios realicen operaciones cotidianas de una forma más segura y sin necesidad de tarjetas de débito.

11.2 Reconocimiento facial

Siguiendo con el análisis de los diferentes factores biométricos, no podemos dejar de mencionar al reconocimiento facial, que también puede ser utilizado como segundo factor de autenticación, de hecho Apple, con su sistema de desbloqueo Face ID la de la posibilidad a sus usuarios de efectuar pagos en aplicaciones como el App Store y iTunes Store como también efectuar compras utilizando Apple Pay. El mecanismo de esta tecnología consiste en un sensor de dos partes, una primera parte que proyecta más de 30.000 puntos infrarrojos en el rostro de un ser humano para así ser capaz de obtener una imagen en 3D, el otro módulo lee la imagen resultante y la procesa. Existe una ínfima posibilidad de 1 en 1 millón que alguien pueda desbloquear el teléfono con esta tecnología, mientras que la probabilidad de 1 en 50.000 con las huellas dactilares. [10]

La primera tarea del software de procesamiento es localizar la cara (o caras) dentro de la imagen. Luego se extraen las características faciales. La tecnología de reconocimiento facial se ha desarrollado en dos áreas: métricas faciales y template matching.

La tecnología de métrica facial se basa en la medición de las características faciales específicas (los sistemas generalmente buscan el posicionamiento de los ojos, la nariz y la boca y las distancias entre estas características). También se debe definir el tamaño de las imágenes y la gama de colores. Normalmente, para disminuir la carga computacional del sistema, se acostumbra a utilizar imágenes pequeñas en escala de grises. A veces también se realiza una ecualización del histograma. [14]

En el template matching se utilizan modelos de comparación para el reconocimiento. El problema es que hay que comparar muchas características (un pixel por ejemplo), y si tenemos en cuenta que en la base de datos encontramos M personas, con N imágenes por persona, observamos que este método no se puede implementar en tiempo real. Por lo tanto, se trabaja con otros métodos que correlacionan las características entre sí para conseguir reducir el espacio facial en un número menor de coeficientes, que tengan un alto poder discriminatorio entre las personas. [14][15]

Siguiendo con la idea de identificar factores de autenticación, tenemos aquellos factores biométricos que utilizan a los ojos para podernos identificar debido a que ellos permanecen casi intactos durante la vida de una persona. Algunos métodos utilizan la retina iluminando los complejos vasos sanguíneos del ojo de una persona utilizando luz infrarroja, haciéndolos más visibles que el tejido circundante. Otros utilizan el iris tomando fotos o videos de alta calidad de cada uno de ellos.

11.2.1 Retina

Como dijimos antes, la exploración de la retina se basa en el patrón de los vasos sanguíneos en la retina del ojo. Esta tecnología de escaneo es más antigua que la tecnología de escaneo de iris que también usa una parte del ojo. [14]

El principal inconveniente del escaneo de retina es su intrusión. El método para obtener una exploración de retina es personalmente invasivo. Se debe dirigir una luz láser a través de la córnea del ojo. Sumado a esto, el

funcionamiento del escáner de retina requiere un operador experto y la persona que se escanea debe seguir sus instrucciones.

Se dice que los sistemas de exploración de la retina son muy precisos aunque tienen una tasa alta de falsos negativos o FRR, ya que no siempre es fácil capturar una imagen perfecta de la retina.

Hoy en día es muy difícil verlo en funcionamiento ya que no es fácil de usar y sigue siendo muy costoso. Es adecuado para aplicaciones donde se requiere alta seguridad y la aceptación del usuario no es un aspecto importante. Los sistemas de escaneo de retina se utilizan en muchas cárceles de EEUU Para verificar a los prisioneros antes de que sean liberados.

11.2.2 Iris

El iris es el anillo coloreado de tejido texturizado que rodea la pupila del ojo. Incluso los gemelos tienen diferentes patrones de iris, además el iris izquierdo y derecho de cada persona también es diferente. Diferentes investigaciones muestran que la precisión de la identificación del iris es mayor que la de las pruebas de ADN. [14]

El patrón del iris lo toma una cámara especial de escala de grises a una distancia de 10 a 40 cm del ojo humano (los modelos anteriores de escáneres de iris requerían un posicionamiento ocular más cercano). No necesita condiciones especiales de iluminación ni ningún tipo especial de luz (a diferencia de la luz infrarroja necesaria para el escaneo de retina). Su tecnología de escaneo no es intrusiva y, por lo tanto, la mayoría de los usuarios la considera aceptable. El patrón del iris permanece estable durante la vida de una persona, y solo se ve afectado por varias enfermedades.

11.3 Reconocimiento de voz

El reconocimiento de voz es algo que evoluciono estos últimos años, si bien el micrófono ya era un dispositivo económico y estaba equipado en casi cualquier computadora o celular, el software de reconocimiento todavía no estaba explotado. Con la aparición de asistentes como Cortana, Siri,

Alexa y Google Now, que intentan reconocer que es lo que está diciendo una persona, se logró dar un gran paso. El siguiente paso es saber quién lo está diciendo, lo que muchos investigadores llaman el reconocimiento del orador. Esta técnica genera huellas de voz e identifica a una persona en cuestión, no solo utilizando la voz como tal, sino que también por las expresiones que utiliza, el uso del lenguaje, vocabulario y la gramática. Se centra en las características vocales que producen el habla que dependen de las dimensiones del tracto vocal, la boca, las cavidades nasales y los otros mecanismos de procesamiento del habla del cuerpo humano. [13][14]

El sistema generalmente le pide al usuario que pronuncie una frase durante el registro, la voz se procesa y se almacena en una plantilla (huella de voz). Más tarde, el sistema solicita la misma frase y compara las huellas de voz. Tal sistema es vulnerable a los ataques de repetición si un atacante registra la frase del usuario y la reproduce más tarde. Los sistemas más sofisticados utilizan un protocolo de desafío-respuesta. Durante la inscripción, el sistema registra la pronunciación de múltiples frases desafío-respuesta (por ejemplo, números). Luego en la fase de autenticación, el sistema elige aleatoriamente un desafío y le pide al usuario que lo pronuncie. En este caso, el sistema no solo compara las huellas de voz, sino que también implementa los algoritmos de reconocimiento de voz y comprueba si realmente se ha dicho el desafío adecuado. [15]

En España ya es utilizado por algunas entidades como Bankia, para garantizar que son sus empleados quienes están intentando cambiar sus contraseñas, o BME para la firma de contratos. Otro ejemplo es Nuance, una empresa que lleva bastantes años trabajando en el ámbito del reconocimiento de voz, han desarrollado un motor de reconocimiento biométrico que a través de una frase como “mi voz es mi contraseña”
permite a los usuarios identificarse en un servidor de forma segura y cifrar su conexión con un algoritmo mucho más avanzado y seguro que el que puede ofrecer un pin o una contraseña.

11.4 Comportamiento del usuario

Otro de los métodos biométricos que se está desarrollando es el comportamiento del usuario con diferentes periféricos como el ratón, teclado o una pantalla táctil que hablan de una persona unívocamente por la velocidad de escritura, la fuerza de tecleo, la duración de la pulsación, el periodo de tiempo que pasa entre que se presiona una tecla y otra, la velocidad a la hora de mover el ratón y hasta el lenguaje utilizado cuando se escriben emails.

La principal ventaja de esta técnica es que la inversión necesaria en sensores es prácticamente nula, ya que estos periféricos están presentes en múltiples aspectos de nuestra vida cotidiana y además altamente aceptados por la población, que hace uso de ellos a diario. De este modo el costo de implantación se centraría principalmente en el software. [11]

Una de las aplicaciones más cercanas para este segundo factor es el e-commerce, ya que se podría pensar que mientras buscas productos y navegas por los sitios de compra estás haciendo clic, moviendo el cursor y utilizando el teclado, todo esto puede servir para identificarte y hacer un checkout más amigable.

11.5 Otros factores biométricos

Existen otros métodos para la identificación biométrica como el movimiento corporal o la cadencia del paso, que hace referencia a la forma de caminar de una persona. Un ejemplo es el sistema Gait Recognition desarrollado por la empresa china Watrix, que utiliza inteligencia artificial para reconocer la forma del cuerpo y el estilo de andar de los seres humanos e identificarlo incluso si su rostro está cubierto o cuando están caminando con la espalda hacia la cámara. [14][15]

El reconocimiento de la geometría de la mano es otro factor muy utilizado. Esta tecnología utiliza la forma de la mano para confirmar la identidad del individuo. Para la captura de la muestra se emplean una serie de cámaras que toman imágenes en 3D de la mano desde diferentes ángulos. Las características extraídas incluyen las curvas de los dedos, su

grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general. No se tienen en cuenta detalles superficiales, tales como huellas dactilares, líneas, cicatrices o suciedad, así como las uñas, que pueden variar de tamaño en un breve período de tiempo. Si bien es cierto que la estructura de los huesos y las articulaciones de la mano son rasgos relativamente constantes, no obstante otras circunstancias, como una inflamación o una lesión, pueden variar la estructura básica de la mano dificultando la autenticación.

En el anexo 1 van a poder encontrar una tabla (Tabla 1) donde muestra una comparación entre algunos de los diferentes sistemas biométricos existentes, midiendo para cada caso la fiabilidad, facilidad de uso, prevención de ataques, aceptación y estabilidad.

11.6 Ventajas frente a otros factores

La implantación de tecnologías biométricas conlleva un conjunto de ventajas frente a otros factores de autenticación. Sin duda, una de las ventajas más importantes para las empresas de la utilización de técnicas biométricas es para la autenticación de empleados, garantizando así que la persona es quien dice ser, es decir, que los rasgos biométricos se encuentran exclusivamente ligados a su legítimo usuario en un horario determinado. Mediante el robo de credenciales o tarjetas identificativas, un individuo puede acceder a zonas restringidas o realizar operaciones no permitidas, inculpando a terceros. Asimismo, es posible que estas credenciales se compartan voluntariamente entre empleados. A través de la implementación de sistemas biométricos, se aumenta la seguridad reduciendo la probabilidad de que alguien no autorizado acceda a zonas o a aplicaciones restringidas. [15]

Las tecnologías biométricas surgen como alternativa o complemento a las técnicas de identificación y autenticación existentes. Por ello es posible establecer una comparación directa entre ambas, destacando beneficios que resultan del uso de biometría junto con aspectos en los que las técnicas tradicionales son superiores: [15]

- Necesidad de secreto: las contraseñas han de ocultarse y las tarjetas no deben de estar al alcance de terceros, mientras que la biometría no requiere de estas medidas de protección que son exclusivamente dependientes del usuario.
- Posibilidad de robo: las tarjetas y contraseñas pueden ser robadas. Sin embargo, robar un rasgo biométrico es extremadamente complejo.
- Posibilidad de pérdida: las contraseñas son fácilmente olvidables y las tarjetas se pueden perder. Los rasgos biométricos permanecen invariables salvo en contadas excepciones y siempre están con el sujeto a quien identifican.
- Comodidad del usuario: el usuario ha de memorizar una o múltiples contraseñas y, en el caso de que use una tarjeta, ha de llevarse siempre consigo. Utilizando tecnología biométrica no se necesita realizar estos esfuerzos.
- Coste de mantenimiento: el coste de mantenimiento de un sistema biométrico, una vez está implantado con éxito, es menor al de un sistema de contraseña o tarjeta ya que no conlleva gastos de gestión asociados a la pérdida u olvido de credenciales.

11.7 No todo es perfecto

Al igual que con todos los factores de autenticación, existen riesgos asociados con la biométrica, incluidos falsos positivos y datos comprometidos. Si bien tienen muchas ventajas como antes mencionamos, los sistemas de autenticación biométrica tienen algunos problemas importantes a tener en cuenta, lo cuales mencionaremos a continuación. [15]

11.7.1 Son Únicos, Permanentes e Irrevocables

Aunque una de las ventajas de los sistemas biométrico es que obtiene rasgos únicos e intrínsecos a cada persona, esto al mismo tiempo es una desventaja, ya que no pueden ser reemplazados, lo que implica que una vez alguien es capaz de replicarlos no es posible revocarlos y obtener uno nuevo al igual que con una contraseña o un token.

Al haber sido comprometida por ejemplo, nuestra huella dactilar, podría ser usada para acceder a cualquier otro servicio o dispositivo en el que haya sido utilizada como credencial, lo que rompe con dos de las máximas en seguridad: utilizar una contraseña diferente para cada servicio o dispositivo (de forma que si alguien compromete uno de ellos, no pueda acceder al resto) y cambiarlas regularmente.

Desde Alemania, miembros del Chaos Computer Club lograron falsificar el lector de huellas dactilares TouchID del iPhone en menos de dos días desde su lanzamiento. Para desbloquear el iPhone 5s, los integrantes del grupo simplemente utilizaron una huella dactilar fotografiada en una superficie de vidrio.

El desafío radica en que los escáneres biométricos, incluidos los sistemas de reconocimiento facial, no son infalibles. Investigadores de la Universidad de Carolina del Norte en Chapel Hill descargaron fotos de 20 voluntarios de redes sociales y las utilizaron para construir modelos 3D de sus rostros. Los científicos lograron vulnerar la seguridad de cuatro de los cinco sistemas de seguridad analizados.

11.7.2 Son públicos, y su obtención es relativamente sencilla

A diario dejamos nuestras huellas impresas en todas partes, las cámaras fotográficas y videocámaras actuales disponen de una gran resolución y sus ópticas permiten hacer zoom a grandes distancias, por lo que cualquier persona puede disponer de equipamiento para fotografiar nuestros ojos en la calle, desde grandes distancias y con un nivel de detalle excepcional.

La voz de una persona puede ser grabada fácilmente en un bar, a través del teléfono o una videoconferencia, y con el equipo adecuado, desde grandes distancias. La tecnología de reconocimiento y síntesis de voz está muy avanzada, y existen programas software (inicialmente diseñados para la industria musical) que permiten sintetizar frases nuevas a partir de unas cuantas sílabas sueltas, emulando incluso diferentes inflexiones y timbres vocales.

El movimiento corporal y expresiones faciales son fácilmente capturables con tecnologías como las utilizadas en el cine (Markerless Mocap: captura de movimiento sin marcadores), o los videojuegos (Xbox Kinetic, PlayStation Eye), hoy en día accesibles fácilmente a cualquier persona.

El desafío radica en que los escáneres biométricos, incluidos los sistemas de reconocimiento facial, no son infalibles. Investigadores de la Universidad de Carolina del Norte en Chapel Hill descargaron fotos de 20 voluntarios de redes sociales y las utilizaron para construir modelos 3D de sus rostros. Los científicos lograron vulnerar la seguridad de cuatro de los cinco sistemas de seguridad analizados.

11.7.3 No se pueden denegar

Memorizando una contraseña, es muy difícil que alguien pueda forzar a otra persona a revelarla contra su voluntad. Ya sea con una negación explícita, o utilizando la negación plausible (generando una situación en la que es imposible demostrar lo contrario, como “no la recuerdo” o “no la conozco”).

Sin embargo, sí es posible ser forzado físicamente a utilizar nuestro dedo para desbloquear un acceso, por lo que el empleo de este tipo de autenticación añade una amenaza, no solo a la seguridad de la información, si no a la integridad física de la persona, que podría ser agredida o secuestrada para obtener sus credenciales.

11.7.4 Pueden ser robados por medios fuera del control del propietario

La información extraída de un rasgo biométrico debe ser almacenada en algún tipo de base de datos, independientemente del formato que se utilice. Esto abre las puertas a que no solo se puedan robar físicamente, sino también comprometiendo el lugar donde se almacenan esos datos, ya sea:

- Con ingeniería inversa sobre el dispositivo electrónico donde se almacena (microchip, memoria, etc)

- Comprometiendo la seguridad de un servidor o base de datos donde pudiese estar guardada.

No sería necesario obtener la imagen de una huella, puesto que los datos extraídos y almacenados de ella (ya sean patrones, geometría o hashes) son potencialmente susceptibles de ser utilizados, o bien para ser inyectados directamente en el sistema sin pasar por el sensor, o para, previo análisis del algoritmo de generación, realizar una reconstrucción de la misma.

El pasado agosto de este año se detectó que la empresa Biostar 2 que utiliza huellas dactilares y reconocimiento facial como parte de sus medios para identificar a las personas que intentan acceder a los edificios tenía una falla de seguridad en sus sistemas que permitió a los investigadores tener acceso a más de 27,8 millones de registros y 23 gigabytes de datos, incluidos paneles de administración, tableros, datos de huellas digitales, datos de reconocimiento facial, fotos faciales de usuarios, nombres de usuario y contraseñas sin cifrar, registros de acceso a las instalaciones, niveles de seguridad y autorización, y detalles personales del personal[9].

[9] Se puede ver más información sobre el caso Biostar 2 en https://www.vpnmentor.com/blog/report-biostar2-leak/

12 Vulnerabilidades de los MFA

Si bien son los sistemas de MFA son más seguros que los mecanismos de autenticación simple, éstos no son infalibles. Existen muchos tipos de ataques y de hecho muy ingeniosos para poder burlar a estos sistemas. A continuación veremos diferentes casos en donde han sido vulnerados:

12.1 Ataque SS7

Los cibercriminales pueden acceder a tus mensajes de distintas formas y una de las más extravagantes es explotando un error en el protocolo SS7 utilizado por las compañías de telecomunicaciones para coordinar el envío de mensajes.

Se trata de un conjunto de protocolos de señalización telefónica empleado en la mayor parte de redes telefónicas mundiales. Su principal propósito es el establecimiento y finalización de llamadas. También tiene otros usos, entre los que se destacan la traducción de números, mecanismos de tarificación prepago y envío de mensajes cortos (SMS).

A la red SS7 no le importa quién envía la solicitud, por tanto, si alguien consigue acceder, la red seguirá sus comandos como si fueran legítimos para dirigir los mensajes y llamadas.

En el año 2008 se publicaron varias vulnerabilidades que presentaba este protocolo que permitía a un atacante hacer un seguimiento del dispositivo móvil sin que el usuario lo supiera. En 2014 también se encontró una vulnerabilidad que permitía la escucha y la lectura de mensajes de texto para ello se apoyaba en el reenvío de llamadas. En 2016 se publica una vulnerabilidad que puede ser aprovechada para hacerse pasar por otra persona y leer los mensajes privados en WhatsApp y Telegram. Aprovenchan que estos servicios utilizan SMS para una verificación de la autenticación. El ataque consiste en hacer creer a la red telefónica que el teléfono del atacante tiene el mismo número que el teléfono del atacado.

Esto permite al atacante recibir el código que le permite verificarse como un receptor válido. [17]

En el año 2017, O2 Telefónica, un proveedor de servicio móvil alemán, confirmó que cibercriminales había explotado vulnerabilidades SS7 para eludir autenticación con dos factores para realizar extracciones de dinero de cuentas bancarias. Los criminales primero instalaban un troyano en los ordenadores de los usuarios. De esta forma robaban credenciales en línea de cuentas bancarias y números de teléfono. A continuación el atacante redirigía el número de teléfono de la víctima a una línea controlado por él. Finalmente el atacante entraba a la cuenta de la víctima y transfería el dinero a una cuenta controlada con él. El banco realizaba una llamada de confirmación pero esta era interceptada por el móvil que controlaba fraudulentamente el número de línea del usuario. [17]

Esta vulnerabilidad expone a aquellos sistemas que utilizan mecanismos de verificación de dos pasos implementado con mensajes SMS o llamadas telefónicas como forma de enviar el código OTP al celular de la víctima, permitiendo a un atacante interceptar el mismo.

12.2 Skimmers

Los skimmers son dispositivos electrónicos que son colocados en aquellas maquinas que tienen una entrada de tarjeta de crédito, como por ejemplo un cajero automático, una estación de carga automática de combustible para engañar a las personas que lo utilizan.

Ilustración 11: lector de tarjeta y teclado falso para robar los dos factores de autenticación

Existen variedades de formas y metodologías de operación pero básicamente copian los datos de la tarjeta magnética y obtienen el pin del usuario. El más común es

colocar un lector falso por sobre el verdadero, de manera que el usuario que opera no se dé cuenta del fraude, este lector almacena los datos en una memoria interno o los envía al exterior, luego una cámara oculta ó un teclado falso captura el pin ingresado, de esta manera el delincuente se hace con los datos de los dos factores.

En cuanto a la conectividad existen 3 tipos de skimmer:

- No conectados: aquellos que tienen una memoria interna y para extraer la información deben ser retirados de donde fueron colocados.
- Corto alcance: son aquellos que envían los datos vía bluetooth o wifi.
- Largo alcance: aquellos que envían información vía GSM

12.3 Phishing

El termino phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, atacando al eslabón más débil de la cadena de seguridad que es el usuario por lo general enviándole un correo electrónico, o por algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

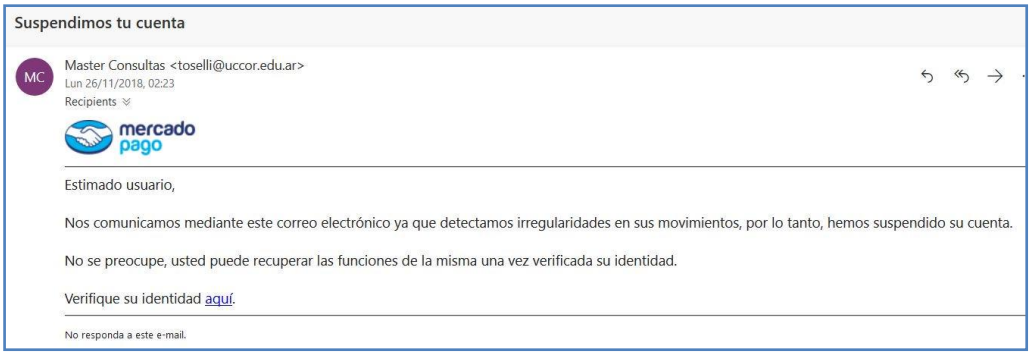


Ilustración 12: ejemplo de phishing vía email teniendo como objetivo datos de la cuenta de Mercado Pago.

Estos correos que son casi idénticos a los legítimos, que suelen mandar las empresas, si vemos la ilustración 12, podemos identificar el phishing mirando en primer lugar el nombre de origen “Master Consultas”, algo que quedo por error de la campaña de phishing anterior. El correo electrónico del emisor toselli@uccor.edu.ar, cuyo dominio no está relacionado con Mercado Pago y por lo que se comprobó después, se trata de un usuario de correo electrónico de la Universidad Católica de Córdoba que le robaron las credenciales y el phisher utilizaba para hacer los envíos, logrando de esta manera que el cliente de correo no lo identifique como un correo no deseado o SPAM.

Los correo contienen links que redirigen al usuario a páginas web clonadas y piden que ingresen no solo su usuario y contraseña, sino que también todos los datos de sus tarjetas de crédito, tarjetas de coordenadas o el token generado aleatoriamente, vulnerando de esta manera a los dos factores de autenticación utilizadas por muchas instituciones.

Observando la URL del link es otra forma de identificar el phishing, aunque no es una garantía, ya que existen múltiples ataques de suplantación de DNS o DNS Spoofing haciendo que el servidor de nombres resuelva un registro de resultados incorrectos, por ejemplo, una dirección IP, desviando el trafico al servidor del atacante.

Piotr Duszyński un investigador polaco desarrollo y publico a principios de este año en Github a Modlishka[10], una herramienta que permite automatizar los ataques de phishing incluso para sitios que utilizan 2FA. Esta herramienta funciona como un proxy reverso modificado para manejar el tráfico destinado a páginas de inicio de sesión y operaciones de phishing. Se ubica en el medio entre la víctima y el sitio, evitando la necesidad de realizar plantillas o clonaciones de un sitio. Cualquier contraseña que pueda ingresar un usuario se registra automáticamente en el panel de backend de Modlishka, mientras que el proxy inverso también solicita a los usuarios tokens 2FA. Si los atacantes están disponibles para recolectar estos tokens 2FA en tiempo real, pueden usarlos para iniciar sesión en las cuentas de las víctimas y establecer sesiones nuevas y legítimas.

12.4 Clonación de huellas dactilares

En enero del 2017 todo el mundo se revolucionó con una noticia sobre un estudio llevado a cabo por investigadores del Instituto Nacional de Informática de Japón[11], que afirmaba que pueden clonarse las huellas dactilares a través de una fotografía en la que un sujeto pose mostrando sus dedos y se encuentre a una distancia de hasta tres metros del objetivo.

Este descubrimiento nos puso a pensar sobre el peligro de subir imágenes a Internet en las que las manos adopten formas como el símbolo de la paz, la victoria o el popular saludo de StarTrek, ya que haría posible la reproducción de la huella dactilar para su uso en sensores biométricos.

Si bien esto se demostró, es cierto que es necesario reunir ciertas condiciones para que esto suceda, como la perspectiva de la foto, el ángulo en la que fue tomada, la calidad de las mismas (mucha redes sociales comprimen la foto antes de subirla), entre otras. Por otro lado la clonación de huellas es algo que también sucede con lectores falsos, que recogen esa información y luego la utilizan para replicarla. Se utilizan resinas, plastilina y hasta impresoras 3D para replicar las huellas.

[10] Se puede descargar la herramienta desde este link: https://github.com/drk1wi/Modlishka
[11] Más información sobre el estudio en https://www.yahoo.com/tech/japan-researchers-warn-fingerprint-theft-peace-sign-101451701.html

Este año Aerolíneas Argentinas echó a seis empleados luego de descubrir una maniobra ilícita que llevaban a cabo y consistía en falsificar su ingreso durante varios días a la semana por medio de un dispositivo de dedos de silicona con el que registraban su asistencia al lugar de trabajo. La operatoria de los cesanteados era la siguiente: se turnaban para que solo uno de los seis acudiera al trabajo. Este llevaba consigo artefactos de silicona de color blanco, que tenían impresos las huellas de los otros cinco y con los que sorteaban el control de acceso biométrico.

12.5 Otros

Existen otras formas de burlar al segundo factor, cada vez más inteligentes:

- Notificaciones activadas: las notificaciones en los smartphone son aquellas que aparecen en la pantalla de nuestro celular avisándonos de aquellas cosas que creemos importantes, se pueden ver sin que el celular este desbloqueado. Esta funcionalidad generalmente viene activada por defecto podría es utilizada por alguien para leer el código OTP que nos enviaron vía SMS o email.
- Troyanos: existen troyanos que pueden leer los mensajes SMS, hacer capturar pantallas, entre otras pudiendo acceder al OTP que nos enviaron.

13 La alianza FIDO y sus protocolos

La Alianza FIDO (Fast IDentity Online) es una asociación entre industrias del sector tecnológico con una misión enfocada: construir estándares abiertos de autenticación para ayudar a reducir la excesiva dependencia del mundo de las contraseñas. Fue construida en el año 2013 para abordar la falta de interoperabilidad entre los dispositivos de autenticación fuerte y los problemas que enfrentan los usuarios al crear y recordar múltiples nombres de usuario y contraseñas. Nok Nok Labs, PayPal y Lenovo estuvieron entre los fundadores, aunque hoy en día también forman parte grandes empresas del mundo tecnológico. [18][19]

Todos los protocolos de FIDO están basados en criptografía de clave pública, es por eso que es importante introducir algunos conceptos.

La criptografía de clave pública o criptografía asimétrica fue inventada en la década de 1970, solución al problema de los secretos compartidos. Es un pilar de la seguridad moderna de internet; por ejemplo, cada vez que nos conectamos a un sitio web HTTPS o firmamos un documento digitalmente. [18]

La criptografía de clave pública utiliza el concepto de un par de claves; una clave privada que se almacena de forma segura con el usuario y una clave pública que se puede compartir con el servidor. Estas claves son números largos y aleatorios que tienen una relación matemática entre sí y permite solo al propietario de la clave privada descifrar algo encriptado con la pública. Veremos más adelante en detalle el uso de estos conceptos.

Ahora repasaremos algunos de los protocolos más importantes desarrollados por la FIDO Alliance que terminan evolucionando en la nueva especificación FIDO2, publicada en marzo de 2019 y aceptada como estándar por la W3C:

13.1 Universal Second Factor (U2F)

Como su nombre lo indica es un estándar universal para la autenticación de dos factores, mediante el uso de una clave USB o un dispositivo con una antena NFC. [19]

Los dispositivos USB se comunican con la computadora host mediante el protocolo del dispositivo de interfaz humana (HID), imitando un teclado. Esto evita la necesidad de que el usuario instale un software de controlador de hardware especial en la computadora host, y permite que el software de aplicación (como un navegador) acceda directamente a las funciones de seguridad del dispositivo sin el esfuerzo del usuario, aparte de poseer e insertar el dispositivo. Una vez que se establece la comunicación, la aplicación ejerce una autenticación de desafío-respuesta con el dispositivo utilizando métodos de criptografía de clave pública y una clave de dispositivo única secreta que se integró en el dispositivo. La clave del dispositivo está protegida contra la duplicación por un grado de confianza social en el fabricante comercial, y se protege lógicamente contra la ingeniería inversa o la falsificación por la robustez del cifrado y la posesión física. [19]

La principal desventaja que presentaban estos estándares era la compatibilidad de los navegadores como Google Chrome, Firefox y Opera, ya que necesitaban que estos reaccionen al insertar la llave. Esto hoy en día ya no es un problema debido a que los principales navegadores son compatibles con este tipo de dispositivos, por lo que si usamos una versión reciente, podremos usar estas llaves sin problemas. [19]

Existen varias plataformas web que son compatibles con estas llaves U2F, como, por ejemplo, Facebook, Twitter, Dropbox, GitHub, Google, Windows, Linux, MacOS, AWS entre otros, y cada vez más plataformas lo están sumando a implementar esta forma de autenticación.

13.1.1 ¿Cómo funcionan?

Estas llaves utilizan algoritmos de cifrado asimétrico, generalmente de exponenciación modular como el conocido RSA, Diffie Hellman, El Gamal, entre otros. En su interior genera las dos claves con números primos

extremadamente grandes necesarias para operar: pública y privada. La clave pública es compartida con el verificador, quien la almacena en sus servidores para utilizarla en el momento de la comprobación de identidad. Entonces, una vez que se pasa por la primera autenticación, utilizando generalmente contraseñas, se le pide al usuario que introduzca el dispositivo USB (muchos de ellos poseen un botón para lograr que se ejecute esta acción). La única forma de poder autenticarse es utilizando la clave privada, y lo mejor es que todo esto se realiza en unos segundos sin interacción del usuario. [18][19]

13.2 Universal Authentication Framework (UAF)

Permite la autenticación de un usuario sin contraseñas, a través de un dispositivo que tenga las funcionalidades de UAF instaladas. La autenticación se logra utilizando algún dato biométrico recolectado por el dispositivo como una huella digital, parámetros de la voz, parámetros de la cámara, entre otras. [19]

Una vez registrado, el usuario simplemente repite la acción de autenticación local cada vez que necesitan autentificarse en el servicio. El usuario ya no necesita ingresar su contraseña cuando se autentica desde ese dispositivo. FIDO UAF también permite combinar múltiples mecanismos de autenticación como huella digital + PIN.

13.3 FIDO2: WebAuthn & CTAP

FIDO2 permite a los usuarios aprovechar dispositivos comunes para autenticar fácilmente los servicios en línea en entornos móviles y de escritorio. FIDO2 se compone de la suma de la especificación de

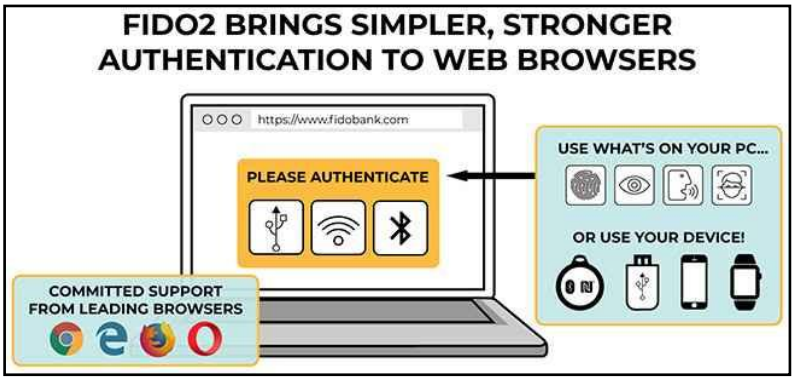


Ilustración 13: muestra las diferentes posibilidades con las cuales un usuario podría autenticarse.

Autenticación Web (WebAuthn) del World Wide Web Consortium (W3C) y el correspondiente Protocolo de Autentificación de Cliente a Autentificador (CTAP) de la Alianza FIDO.

FIDO2 es el sucesor del protocolo FIDO U2F. Posee todas las ventajas de su antecesor con la diferencia que este puede autenticar plataformas de múltiples factores. Se compone de la especificación de autenticación web del W3C y de los correspondientes protocolos de autenticación de cliente (CTAP) de la Alianza FIDO. FIDO2 soporta la autenticación de usuario sin contraseña, de segundo factor y múltiples factores utilizando autenticadores embebidos (como biométricos o PIN) o externos (como las claves de seguridad FIDO, dispositivos móviles, dispositivos portátiles, etc). [19][20]

13.3.1 Client to Authenticator Protocols (CTAP)

CTAP2 permite el uso de autenticadores externos (claves de seguridad FIDO, dispositivos móviles) para la autenticación en navegadores y sistemas operativos compatibles con FIDO2 a través de USB, NFC o BLE para lograr una experiencia de autenticación sin contraseña, de segundo factor o multifactor. [19]

Los sitios web solo almacenan una clave pública, la cual no es secreta, porque es efectivamente inútil sin la clave privada correspondiente. El hecho de que el servidor no reciba ningún secreto tiene implicaciones de largo alcance para la seguridad de los usuarios y las organizaciones. Las bases de datos ya no son tan atractivas para los piratas informáticos, porque las claves públicas no les son útiles.

13.3.2 Web Authentication API (WebAuthn)

WebAuthn es una especificación escrita por W3C y FIDO que permite a los servidores registrar y autenticar a los usuarios utilizando criptografía de clave pública en lugar de una contraseña. [20]

Fue oficialmente fue lanzado en marzo del 2019 y ya es compatible con los principales navegadores y sistemas operativos del mercado como Windows 10, Android, Google Chrome, Mozilla Firefox, Microsoft Edge y Apple Safari. Permite que los servidores utilicen autenticadores fuertes integrados en nuestros dispositivos, como Windows Hello o la identificación táctil de Apple. [20]

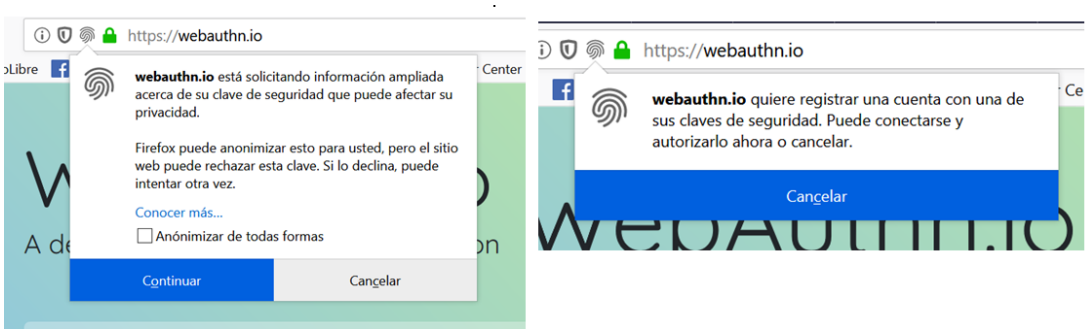


Ilustración 14: ejemplo de implementación de la API WebAuth en navegador Mozilla Firefox corriendo en un sistema operativo Unix.

Las partes intervinientes en este proceso son tres (podemos ayudarnos de la ilustración 15):

- El servidor: también llamado parte confiable, es donde se almacenan los datos del usuario y la clave pública útil para la autenticación.
- El navegador: es donde está el cliente solicitando la operación.
- El autenticador: es el que almacena la clave privada, puede estar integrado en un sistema operativo, como Windows Hello, o puede ser un token físico, como una llave de seguridad USB o Bluetooth.

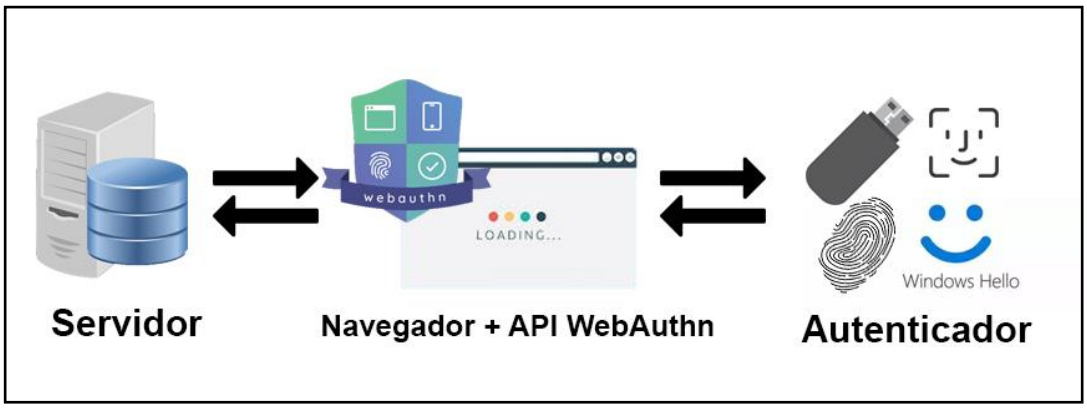


Ilustración 15: flujo de registro y autenticación de WebAuthn

Como mencionamos anteriormente, las operaciones son dos, por un lado el registro es utilizado para la creación de nuevas credenciales de usuario que luego serán útiles en la segunda operación. Estas credenciales son básicamente un par de claves (pública y privada), donde la pública será compartida al servidor y la privada quedará almacenada en nuestro autenticador. [22]

Vamos a ver a continuación el flujo del registro, que se inicia cuando el usuario solicita el registro en un sitio, esta solicitud va por afuera del protocolo de la API de autenticación.

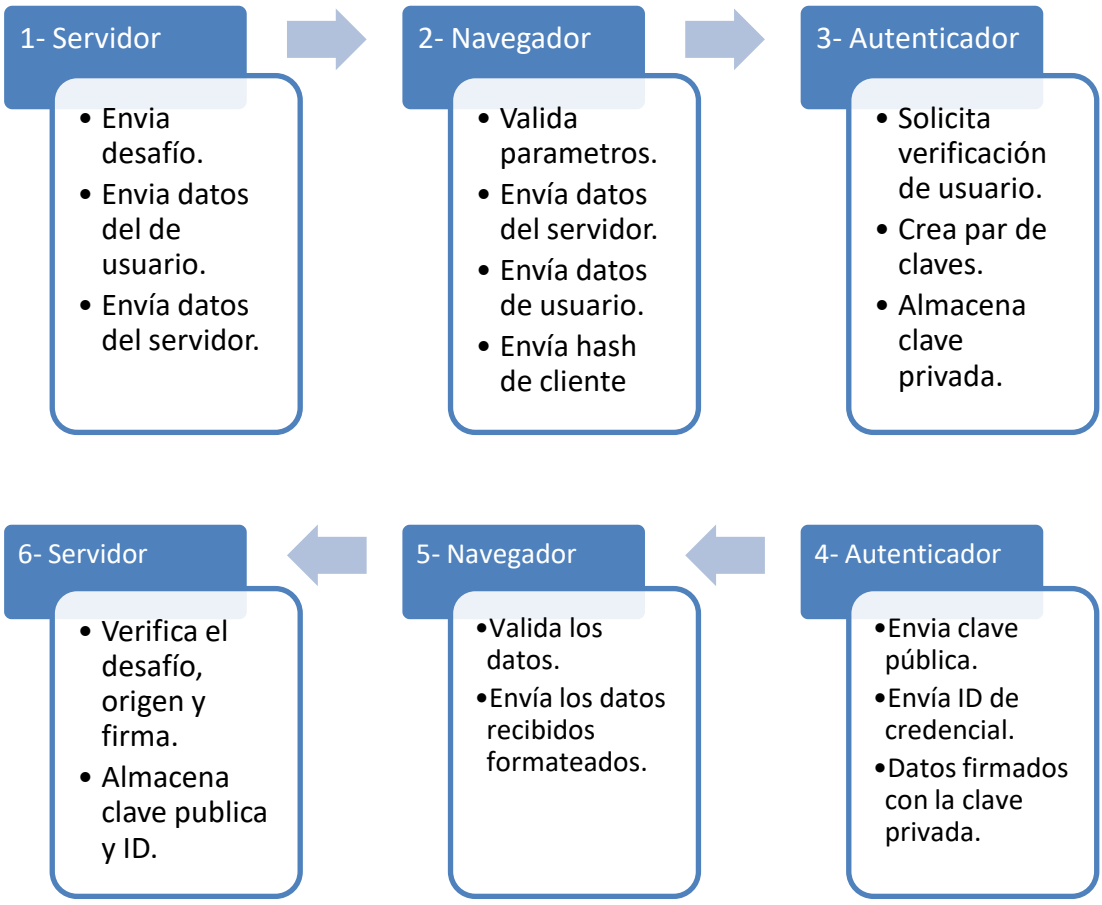


Ilustración 16: proceso de registro con API Aunth.

La segunda etapa es la autenticación, donde se utilizan este par de claves generados anteriormente para validar la autenticación u operación solicitada por el usuario.

Vemos ahora el flujo de autenticación, que es muy similar al de registro. Este también inicia cuando el usuario solicita al servidor la autenticación, siendo la misma una petición que va por fuera del alcance del flujo de la API Aunth:

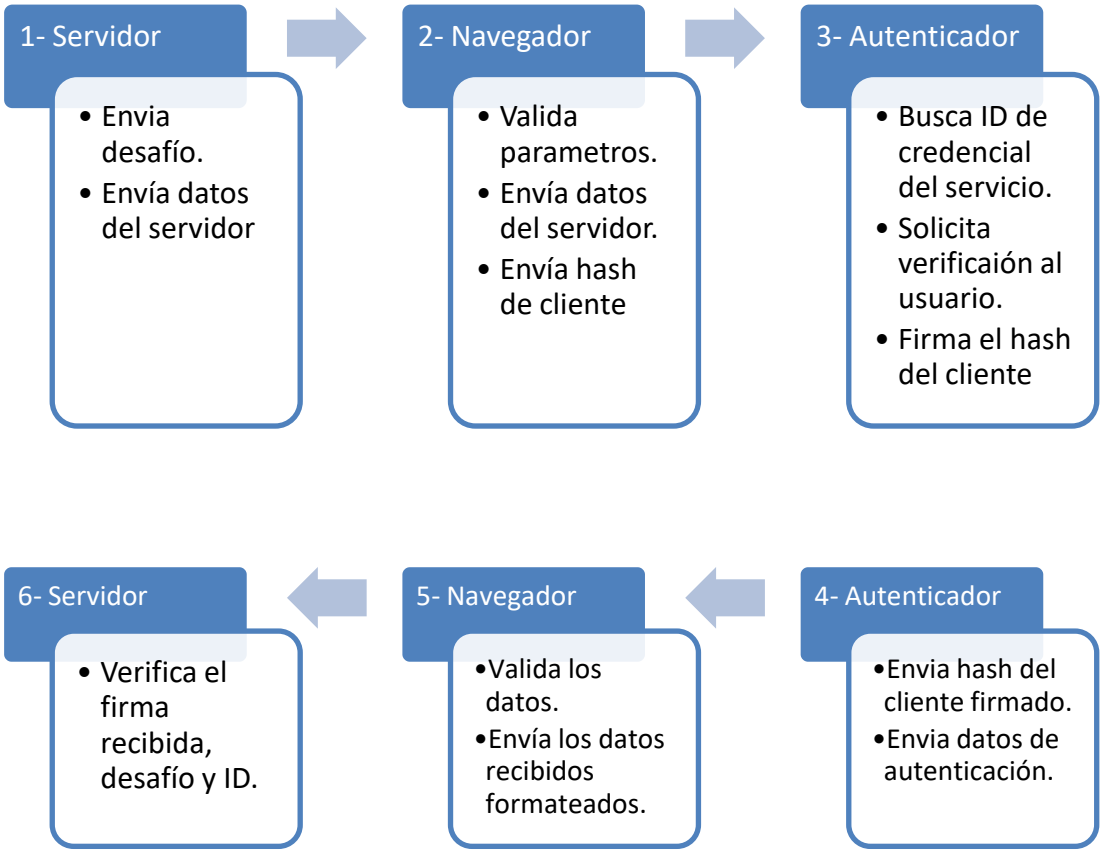


Ilustración 17: Ilustración 16: proceso de autenticación con API Aunth.

Es importante remarcar que todas estas operaciones requieren ser operadas en un contexto seguro, independientemente del protocolo que se utilice. Podría ser REST sobre HTTPS o SOAP seguro, entre otros. [22]

Dejamos en el anexo 2 los pasos para poder implementar la API de WebAuthn en un sitio web y el detalle de las operaciones más importantes.

14 Conclusión

La seguridad en IT siempre fue mal vista por los usuarios, a ellos no les gusta tener que lidiar con las recomendaciones que les damos, con los cuidados que deben tener, con las restricciones que imponemos, con la dificultad que a veces tiene el hecho de realizar ciertas acciones, cuando ellos simplemente quieren enviar un correo electrónico, ingresar a una página web determinada, sacar dinero de un cajero automático, hacer transferencias, ver fotos de sus amigos en alguna red social. Casi siempre somos los malos de la película, aquellos que ponemos palos en la rueda de la productividad ya que les complicamos el uso de las herramientas, hacemos las cosas un poco más difíciles, agregamos un paso más y todo esto en pos de que las mismas sean más seguras. Es de estas situaciones que se popularizó hace años la frase “la seguridad afecta la usabilidad” y creo que esto es falso ya que en la mayoría de los casos, reducir las molestias a los usuarios no hace que algo sea más seguro o viceversa y los esfuerzos para eliminar el uso de las contraseñas es un buen ejemplo de ello.

Si revisamos los orígenes de las contraseñas, cuando las utilizábamos para controlar el acceso una casa en forma de llaves. Los bares clandestinos utilizaban contraseñas para permitir el ingreso solo a las personas que la conocían. Jugar al juego de contraseñas estaba razonablemente bien mientras éramos humanos tratando de evitar que otros humanos entraran a nuestros sistemas; elijo una contraseña secreta y no te la digo. La única forma en que se puede ingresar a mi sistema es tratando de adivinar qué contraseña usé. Al cerebro humano le gustan los patrones simples; la contraseña *"12345"* es fácil de recordar al igual que la palabra *"password"* (ambas son las contraseña más utilizada del mundo). Los equipos de prevención decidieron obligar a los usuarios a usar contraseñas complejas, comenzando una carrera armamentista entre los usuarios y el personal de seguridad de IT, situación bien descripta en la introducción de de este documento. El perdedor: ambos.

¿Qué sucede si se nos ocurre algo que sea fácil para los usuarios pero difícil para las computadoras? Bueno, estamos en ese camino, tan cerca de que las contraseñas desaparezcan de nuestras vidas y no solo para facilitar el ingreso o transacciones a usuarios, sino que aportando al mismo tiempo una solución a grandes problemas actuales de seguridad. Google anuncio en este agosto de 2019 que ya está disponible el acceso a sus cuentas y algunos de sus servicios a través de la autenticación biométrica o pantalla de bloqueo de un smartphone con Android. El director de Estrategia de Seguridad de Nuance, Brett Beranek predice que antes del año 2024 las contraseñas desaparecerán[12] y con los que vimos en este documento no es algo tan descabellado.

[12] Se puede leer mas sobre su opinión en: https://www.businessinsider.es/contrasenas-actuales-desapareceran-antes-2024-segun-este-experto-ciberseguridad-318097

15 Anexo

15.1 Anexo 1: Tabla de comparación de métodos de autenticación biométrica. [5]

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Media	Alta

Tabla 1: comparación entre diferentes métodos de autenticación biométricos.

15.2 Anexo 2: Pasos para autenticación utilizando API WebAuthn [21][22]

A continuación vamos a ver cuáles son los pasos para poder autenticarnos utilizando esta metodología:

15.2.1 Paso 1: el registro

En un flujo de registro de usuario basado en contraseña, un servidor generalmente presentará un formulario a un usuario solicitando un nombre de usuario y contraseña. La contraseña se enviaría al servidor para su almacenamiento. En cambio, en WebAuthn, un servidor debe proporcionar datos que vinculen a un usuario con una credencial (el par de claves). Estos datos incluyen identificadores para el usuario y la organización (también conocida como “la parte confiable"). El sitio web luego usaría la API de autenticación web para solicitar al usuario que cree un nuevo par de claves. Es importante tener en cuenta que necesitamos una cadena generada aleatoriamente desde el servidor como un desafío para evitar ataques de repetición

```
const publicKeyCredentialCreationOptions = {
    challenge: Uint8Array.from(
        randomStringFromServer, c => c.charCodeAt(0)),
    rp: {
        name: "Duo Security",
        id: "duosecurity.com",
    },
    user: {
        id: Uint8Array.from(
            "UZSL85T9AFC", c => c.charCodeAt(0)),
        name: "lee@webauthn.guide",
        displayName: "Lee",
    },
    pubKeyCredParams: [{alg: -7, type: "public-key"}],
    authenticatorSelection: {
        authenticatorAttachment: "cross-platform",
    },
    timeout: 60000,
    attestation: "direct"
};

const credential = await navigator.credentials.create({
    publicKey: publicKeyCredentialCreationOptions
});
```

Ilustración 18: fragmento del código JSON del registro.

Para poder entonces realizar el registro, debemos crear una nueva credencial para un usuario, enviando al servidor la siguiente información:

- **challange**: el desafío es un búfer de bytes criptográficamente aleatorios generados en el servidor, y es necesario para evitar "ataques de repetición".

- **rp**: es "la parte confiable ", puede considerarse como una descripción de la organización responsable de registrar y autenticar al usuario. La identificación debe ser un subconjunto del dominio actualmente en el navegador. Por ejemplo, una identificación válida puede ser *google.com.ar*.
- **user**: esta es información sobre el usuario que se está registrando actualmente. El validador usa la identificación para asociar una credencial con el usuario.
- **pubKeyCredParams**: esta es una matriz de objetos que describe qué tipos de clave pública son aceptados por el servidor. El parametro alg es un número descrito en el registro COSE[13]; por ejemplo, -7 indica que el servidor acepta claves públicas de curva elíptica utilizando un algoritmo de firma SHA-256.
- **authenticatorSelection**: este objeto es opcional, sirve para agregar restricciones sobre el tipo de autenticadores permitidos para el registro. En este ejemplo, estamos indicando que queremos registrar un validador multiplataforma (como un Yubikey) en lugar de un validador de plataforma confiable TPM como Windows Hello o Touch ID.
- **timeout**: el tiempo (en milisegundos) que el usuario tiene que responder a una solicitud de registro antes de que se devuelva un error.
- **attestation**: esta opción permite a los servidores indicar la importancia de los datos de certificación para este evento de registro. Un valor de "none" indica que al servidor no le importa la certificación. Un valor de "indirect" significa que el servidor permitirá datos de certificación anónimos, “direct” significa que el servidor desea recibir los datos de certificación del validador.

El objeto de credencial devuelto por la llamada anterior, es un objeto que contiene la clave pública y otros atributos utilizados para validar el evento de registro. Es aquí donde el navegador o implementador de la API nos solicitará

[13] CBOR Object Signing and Encryption (COSE) es un documento que describe cómo crear y procesar firmas, códigos de autenticación de mensajes y cifrado utilizando CBOR (La representación concisa de objetos binarios) para la serialización. Se puede ver más detalles en: https://www.iana.org/assignments/cose/cose.xhtml

que utilicemos el dispositivo validador que generará el par de claves y se le enviará al servidor la clave pública y el ID de credencial.

Si el proceso de validación tuvo éxito, el servidor almacenaría publicKeyBytes y credentialId en una base de datos, asociada con el usuario.

15.2.2 Paso 2: autenticación

Una vez finalizado el registro, el usuario ahora puede ser autenticado. Durante la autenticación, se realiza una prueba de que el usuario posee la clave privada. Esta afirmación contiene una firma creada usando la clave privada. El servidor utiliza la clave pública recuperada durante el registro para verificar esta firma.

16 Bibliografía

[1] OWASP Fundation. OWASP Top 10. https://www.owasp.org/images/4/46/Proyecto_OWASP.pdf. Edición 2013. (consultado el 28/03/2019).

[2] Aviram Jenik. Helpnet Security. https://www.helpnetsecurity.com/2019/08/01/mandatory-password-changes-are-obsolete/. (consultado el 12/04/2019).

[3] Wikipedia. Multiples Factores de Autenticación - https://es.wikipedia.org/wiki/Autenticaci%C3%B3n_de_m%C3%BAltiples_factores (consultado el 01/05/2019).

[4] María Ángeles Caballero y Diego Cilleros Serrano. El Libro del Hacker. Editorial Anaya. Madrid, 2018.

[5] Alex Drozhzhin. A2F Kapersky daily. https://www.kaspersky.es/blog/2fa-practical-guide/17187/ (consultado el 01/05/2019).

[6] Pablo Alejandro Fain. Autenticación multifactor. https://blog.pablofain.com/2018/08/18/doble-factor-de-autenticacion-y-eso/ (consultado el 05/05/2019)

[7] Wikipedia. FIPS 140-2. https://es.wikipedia.org/wiki/FIPS_140-2. (consultado el 01/05/2019)

[8] Wikipedia. Biometría. https://es.wikipedia.org/wiki/Biometr%C3%ADa. (consultado el 05/05/2019).

[9] Ing. MSc. Gerson Enrique Delgado Parra. https://upload.wikimedia.org/wikipedia/commons/c/ce/Articulo_gerson_delgado_congsistel.pdf. (consultado el 05/05/2019).

[10] Wikipedia. Face ID. https://es.wikipedia.org/wiki/Face_ID. (consultado el 05/05/2019).

[11] Wikipedia. Dinamica de tecleo. https://es.wikipedia.org/wiki/Dinámica_de_tecleo. (consultado el 05/05/2019).

[12] Israa M. Alsaads. Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. International journal of scientific & technology research volume 4. Año 2015.

[13] Alexandre Fustier y Vincent Burger. Biometric authentication. Año 2015.

[14] Zdenek Ríha y Václav Matyáš. Biometric Authentication Systems. Masaryk University. Año 2000.

[15] INCIBE. Tecnologías biométricas aplicadas a la ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf. (consultado el 05/05/2019).

[16] Ana Dascalescu. Biometric Authentication Overview, Advantages & Disadvantages**.** https://heimdalsecurity.com/blog/biometric-authentication/ (consultado el 16/08/2019)

[17] Wikipedia. Sistema de señalización por canal común nro 7. https://es.wikipedia.org/wiki/Sistema_de_se%C3%B1alizaci%C3%B3n_por_canal_com%C3%BAn_n.%C2%BA_7 (consultado el 10/09/2019)

[18] Wikipedia. FIDO Alliance. https://en.wikipedia.org/wiki/FIDO_Alliance (consultado el 05/05/2019)

[19] Dr. Rolf Lindemann Nok. U2F & UAF Tutorial. https://fidoalliance.org/assets/downloads/FIDO-U2F-UAF-Tutorial-v1.pdf. Año 2017. (consultado el 05/05/2019).

[20] Wikipedia. WebAuthn. https://en.wikipedia.org/wiki/WebAuthn. (consultado el 05/05/2019).

[21] WebAuthn. WebAuthn API guide .https://webauthn.guide/. (consultado el 01/06/2019)

[22] Mozilla. WebAuthn API. https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API. (consultado el 03/08/2019)