Escuela Politécnica Superior de Jaén
Máster Universitario en Seguridad Informática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior (Jaén)

Trabajo Fin de Máster

MEJORA EN LA IDENTIFICACIÓN DE USUARIOS BASADA EN BIOMETRÍA

Alumno/a: **Miras Martínez, Rosario**

Tutores: Prof. D. Manuel García Vega
Prof. D. Luis Pablo del Árbol Pérez

Dpto.: Informática

Septiembre, 2021

Agradecimientos

Mi más sincero agradecimiento a todos y todas, y a cada una de las personas que me han prestado su ayuda y colaboración en este trabajo de técnico de investigación, profesores y compañeros y compañeras.

A mi familia, que me ha apoyado y ayudado en tanto en cuanto lo he necesitado y a la que dedico la realización de este Trabajo Fin de Máster.

“En cuestiones de cultura y de saber, sólo se pierde lo que se guarda; sólo se gana lo que se da”, *Antonio Machado*.

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don MANUEL GARCÍA VEGA y Don Luis Pablo del Árbol Pérez, tutores del Proyecto Fin de Máster titulado: MEJORA EN LA IDENTIFICACIÓN DE USUARIOS BASADA EN BIOMETRÍA, que presenta ROSARIO MIRAS MARTÍNEZ, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Septiembre de 2021

El alumno:

Firmado por MIRAS MARTINEZ ROSARIO - 75110225E el día 24/08/2021 con un certificado emitido por AC FNMT Usuarios

ROSARIO MIRAS MARTÍNEZ

El tutor:

GARCIA VEGA MANUEL - 25981567P

Firmado digitalmente por GARCIA VEGA MANUEL - 25981567P
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-25981567P, givenName=MANUEL, sn=GARCIA VEGA, cn=GARCIA VEGA MANUEL - 25981567P
Fecha: 2021.08.25 12:39:48 +02'00'

LUIS PABLO DEL ARBOL PEREZ

Firmado digitalmente por LUIS PABLO DEL ARBOL PEREZ
Fecha: 2021.08.25 13:28:46 +02'00'

MANUEL GARCÍA VEGA

LUIS PABLO DEL ÁRBOL PÉREZ

Índice

1. INTRODUCCIÓN

Este trabajo fin de máster, tiene como principal objetivo, localizar la forma en que un usuario puede identificarse, mediante los puntos de acceso que disponga dicho usuario, intentando siempre hacerlo de la manera más eficaz y eficientemente y con la máxima seguridad posible.

Para ello, se trabajará en el análisis de formas alternativas de identificación de usuarios de forma lo más transparente posible en base a factores de uso y comportamiento de su terminal móvil, con el objetivo de eliminar o, al menos reducir, las desventajas que la identificación tradicional basada en usuario y clave trae consigo.

La identificación de usuarios en el contexto de la informática y la tecnología no es más que la identificación de una persona en un acceso a un sistema, donde para que dicha persona pueda acceder deberá poseer una cuenta. En la mayoría de los casos, esa cuenta estará compuesta por un login y una contraseña. El login es el identificador de usuario, su nombre, y deberá ser único para que identifique biunívocamente a una persona. La contraseña nos autentica en el sistema. Debe estar en posesión sólo del usuario, para que sea segura. Podrá estar compuesta por caracteres alfabéticos o numéricos, caracteres especiales, con un tamaño específico o con una longitud comprendida en un rango establecido. Su configuración la determina el administrador del sistema al que se intenta acceder.

Este sistema de identificación, de login y contraseña, sigue siendo el más extendido por su uso, no así el más seguro [1]. Posee gran cantidad de inconvenientes, pasamos a numerar algunos de ellos:

• La capacidad de los usuarios para recordar largas y variadas contraseñas, ya que el factor olvido en los usuarios está muy presente. Cada día es mayor el número de contraseñas que se gestionan y por tanto el riesgo a olvido o confusión aumenta.

• Uso de contraseñas no fuertes y únicas. Las contraseñas débiles son fáciles de crackear[1] además si son genéricas, es decir, si se mantienen las contraseñas de fábrica que aparecen por defecto o generales, son fácilmente de descifrar.

• Uso de la misma contraseña para todas las aplicaciones y/o servicios. Es un error muy común y se pone en peligro todos los servicios y/o aplicaciones de un mismo usuario, por lo que se recomienda no usar la misma contraseña para todo.

• Acceso a sitios oficiales seguros, ya que hay multitud de sitios y/o aplicaciones que se esconden bajo un aspecto seguro con el único precepto de robar las credenciales de un usuario.

• Aumento de técnicas empleadas por los ciberdelincuentes para obtener contraseñas. Ataques Man-in-the-middle, sistemas de keyloggers, Ingeniería social, envíos masivos de email o phishing, Botnets, …

Tras detectarse en el sistema de identificación ataques de fuerza bruta [2] mediante posibles identificaciones de sistemas automáticos, es decir, mediante máquinas, a principios del año 2000, para aumentar la seguridad en la identificación de usuarios con login y contraseña, empezaron a usarse varios factores complementarios que dotarían al proceso de robustez. El primer factor que apareció fue la herramienta “Captcha”[2], que intenta descartar que el proceso de identificación lo está realizando una persona o una máquina. Es una herramienta muy simple que consta de una secuencia aleatoria de letras o números que aparecen visiblemente borrosos y una caja de texto donde se debe introducir dicha secuencia. La introducción de un Captcha en el proceso de identificación elimina la posibilidad de entradas remotas, como el ataque de fuerza bruta, o protección contra Spam, y dificulta el reconocimiento por parte de

[1] https://www.researchgate.net/profile/Cm-Legon/publication/331135825_Characterization_of_an_attacker_to_password_authentication_Systems_Caracterizacion_de_un_Atacante_a_sistemas_de_Autenticacion_por_Contrasenas/links/5c6739a5299bf1e3a5abe4e4/Characterization-of-an-attacker-to-password-authentication-Systems-Caracterizacion-de-un-Atacante-a-sistemas-de-Autenticacion-por-Contrasenas.pdf

[2] https://support.google.com/a/answer/1217728?hl=es

aplicaciones OCR. A medida que comenzó a usarse, empezaron a detectarse las primeras debilidades: posibilidad de reconocimiento de caracteres mediante aplicaciones OCR más sofisticadas o reutilización de ID de sesión de otra imagen captcha conocida. La herramienta siguió evolucionando y en 2009 Google lanzó Recaptcha [3], donde el sistema aumentaba a dos las palabras que debían de introducirse en el recuadro de texto. Una de las palabras era conocida por el sistema mientras que la otra palabra eran caracteres imposibles de reconocer por un OCR. La inteligencia artificial siguió evolucionando y con ella las maneras de saltarse estos controles, por lo que Google lanzó en 2014 la versión 2 llamada No Captcha Recaptcha. Esta nueva versión añadía la opción “no soy un robot”. Al pinchar se abrirá una ventana donde se deberán hacer clic sobre algunas imágenes. Seguía la evolución y a finales de 2018 nació la última versión llamada Recaptcha invisible (Recaptcha v3) [4], la cual pretende que el usuario no tenga que hacer nada extra, es decir, se base en patrones de comportamiento sobre la interacción del usuario en las páginas web. En la actualidad el proceso de Captcha está disponible para discapacitados visuales, donde hay posibilidad de escuchar un audio. Pero en contra, aun no existe una versión para la comunidad sordociega.

Otra medida que mejoraba la seguridad en la identificación de usuarios frente a los ataques de fuerza bruta o posibles ataques dirigidos automáticamente provenientes de una máquina fue la limitación de intentos para introducción de contraseñas. Si cada vez que se tiene que volver a introducir una contraseña tras una contraseña errónea previa se introduce un retardo de tiempo, se elimina la posibilidad de ataques dirigidos. Como el tiempo de retardo va en aumento conforme aumenta el número de intentos, llega un momento en que es inviable estos tipos de ataques.

Está claro según lo expuesto anteriormente, que toda medida es poca para evitar estos tipos de ataques dirigidos, por lo que cuantas más medidas de las anteriormente citadas combinemos, mayor será la seguridad. La unión hace la fuerza.

La tecnología avanzaba a medida que avanzaban los años y a finales del siglo XX empezaron a aparecer nuevos dispositivos como alternativa de uso de

los tradicionales equipos informáticos. El primero en nacer fue la PDA[3] a mediados de los años 90 las cuales usaban sistemas operativos como Palm OS, Symbian o Pocket PC. HP en 1996 con el modelo OmniGo 700LX fue la primera marca seguida de NOKIA y QUALCOMM. Los sistemas operativos que usaban fueron avanzando y desarrollándose hasta que llegaron los teléfonos inteligentes de uso comercial o smartphone, como ahora es llamado. Nokia lanzó en Europa sus teléfonos con sistemas operativos Symbian y BlackBerry hizo lo mismo en EE. UU. Más tarde llegó Apple, en 2007, con el lanzamiento de IPhone. La era tecnológica avanzaba y fue en 2011 cuando Motorola lanzó el primer teléfono inteligente con lector de huellas dactilares, aunque ha sido a partir del año 2017, con el despegue de IPhone X, cuando ha nacido el reconocimiento facial para identificación de usuarios.

A continuación, nacieron las tabletas y otros dispositivos inteligentes como smartwatches, altavoces inteligentes, en definitiva, una gran variedad de dispositivos IOT[4] que reclamaban conexión a sistemas y acceso a aplicaciones, todo ello conllevando un proceso de autenticación.

Por todo ello aparece el factor de autenticación doble o múltiple factor [5]. Pasamos de “algo que sé”, en el caso anterior era una contraseña, una clave o un pin a “algo que tengo”, como, por ejemplo, una tarjeta de coordenadas o un token.

El segundo factor de autenticación no es más que una capa nueva que complementa a la contraseña que ya teníamos, incrementando notablemente la seguridad. Es decir, refuerza la autenticación de usuario y contraseña, comprobando que el usuario es quien dice ser. Hay varios métodos para aportar ese segundo factor de autenticación [6].

• Uso de SMS como recepción de una clave: presenta como ventaja que el usuario siempre o casi siempre dispone de un teléfono móvil, aunque, por el contrario, esto puede ser un inconveniente, ya que el robo de terminales móviles

[3] https://www.muycomputer.com/2014/07/06/un-trocito-de-historia-evolucion-y-muerte-de-las-pda/
[4] https://www.redhat.com/es/topics/internet-of-things/what-is-iot

está muy presente, además de las vulnerabilidades que presenta el protocolo SS7, usado por la red GSM para el envío de SMS.

• MFA: Autenticación multifactorial. Combina 2 o más factores de autenticación para verificar la identidad de un usuario. Es decir, comprobación de 2 o más pruebas para verificar que es quien dice ser. Algunos de estos factores adicionales pueden ser:

- OTP: Contraseña de un solo uso. Suele ser una cadena de caracteres numéricos o alfanuméricos generados aleatoria y automáticamente.
- 2FA: También llamada autenticación de doble factor o verificación en dos pasos. Proporcionan una capa más de seguridad. En estos procesos de seguridad se utilizan dos factores de autenticación diferentes para verificar la identidad de una persona. Un primer factor sería el uso de una contraseña y como segundo factor se utilizaría un token o un rasgo biométrico.

Tanto para la verificación por MFA como en la recepción de claves en SMS, se necesita que esté presente un terminal móvil. Una amenaza emergente que presentan estos dispositivos es la duplicidad de tarjeta SIM, o también llamada SIM SWAP o Smishing, se intenta obtener información privada a través de un mensaje de texto. Este tipo de incidentes se llevan a cabo mediante la realización de duplicados de tarjetas SIM por parte de los atacantes. Para ello suelen utilizar ingeniería social.

• Tarjetas de coordenadas: son poco aconsejables, y están en desuso en la actualidad ya que son susceptibles a ser pérdidas o robos.

• Aplicaciones OTP: Por ejemplo, Duo Mobile, FreeOTP Authenticator, Latch o Google Authenticator. Son aplicaciones que se instalan en smartphone y producen Token de un solo uso.

Por tanto, aunque existen técnicas para la implementación de un segundo factor de autenticación, no significa que el uso de éste sea un método seguro, debemos conocer las vulnerabilidades y las vías de ataque.

Todo ello nos lleva pensar en que el mayor problema no es otro sino la identificación de los usuarios de la forma más eficaz y eficiente, pero a la vez, la más segura. Como consecuencia, vamos a intentar simplificar dicha identificación, desde todas las formas posibles que pueda tener un usuario.

1.1. Objetivos

Para este TFM se proponen los siguientes objetivos:

1. Análisis de las alternativas que posee un usuario para identificarse desde su terminal móvil o tableta, dependiendo de su uso y su comportamiento con éste.
2. Otro objetivo será que la identificación sea lo más transparente y fácil para el usuario, así como lo más segura posible.
3. Mejora del sistema de identificación de un usuario, usando biometría, ya que, es un sistema de identificación novedoso, al ser transparente al usuario y sin necesidad de su implicación directa, si no que su identificación está basada en su comportamiento físico del uso e interacción con su terminal móvil. Interacciona la posición o localización del usuario, con la forma de coger el terminal más el historial de uso de las aplicaciones de su terminal.
4. Uso de 3 métodos de patrones de comportamiento diferentes que proporcionan y dotan al sistema de identificación un nivel alto de seguridad.
5. Para realizar dicha identificación de los usuarios se ha elegido tres métodos: el sensor GPS y el acelerómetro, que son sensores que están incorporados en los terminales móviles o tabletas, y el historial de uso de las aplicaciones. Los 3 métodos elegidos se basan en patrones de comportamiento del usuario, es decir, son rasgos de comportamiento, características dinámicas que pueden evolucionar y/o modificarse con el paso del tiempo, no son rasgos físicos estáticos. Estos métodos se han elegido de manera que, puedan trabajar en colaboración entre ellos, con una identificación usando sólo dos métodos, o una identificación uniendo los tres métodos elegidos. Además de que son características dinámicas donde su

integración en un prototipo de identificación es eficiente y eficaz al no tener que depender del usuario de manera directa.

2. LA BIOMETRÍA PARA LA IDENTIFICACIÓN Y AUTENTICACIÓN

2.1. Historia cronográfica

No fue hasta el siglo XIX cuando comenzó a usarse la biometría como sistema de identificación. Alphonse Bertillon [7], un médico, policía y antropólogo, introdujo la antropometría para identificar a personas usando diferentes partes del cuerpo. Cabeza, manos, pies, tatuajes, cicatrices, etc. Así, consiguió elaborar una base de datos donde identificó a varios centenares de delincuentes. Aunque más tarde se darían cuenta de la imperfección de este sistema antes dos individuos con iguales características.

Posteriormente, en 1892 de la mano de Juan Vucetich [8], surgió el sistema de identificación usando la huella dactilar. A esta disciplina se le llamó dactiloscopia. Tras analizar la impresión dactilar que dejaban las huellas sobre una superficie planas, vieron que no cabía la posibilidad de que dos huellas dactilares fuesen iguales, ya que cada una, formaban unos valles y unas crestas totalmente diferentes, aunque fuesen de la misma persona y aunque fuesen de la misma mano o pie. En 1904, en un congreso médico, presentó su último trabajo [9], premiado y traducido a varios idiomas, donde más de un siglo después, aún se le sigue considerando.

En 1987, Leonard Flom y Aran Safir [10] consiguieron la identificación mediante iris, pero fue Daughman en 1994, quien patentó los algoritmos de reconocimiento de Iris. Actualmente, propiedad de Iridian Technologies.

El padre del reconocimiento facial fue Woodrow Wilson Bledsoe [11], creando en 1960 la tabla RAND, que no es más que un sistema para clasificar los rasgos del rostro humano. Era todavía un sistema muy rudimentario, ya que había que ir añadiendo las coordenadas horizontales y verticales en una cuadrícula usando un lápiz óptico que emitía pulsos electromagnéticos. Así se registraban las ubicaciones de los ojos, nariz, boca, cabello. Este sistema fue mejorando, y a finales de los 80, gracias a Sirovich y Kirby comenzó a aplicarse el álgebra lineal.

En 1991, Turk y Pentland [12], desarrollan el reconocimiento facial automático capaz de detectar un rostro humano desde una imagen. A partir de esta década, nació el programa FERET, donde se creó una base de datos de imágenes faciales que más tarde se actualizó en 2003 para añadir versiones en color de alta resolución de 24 bits.

En la actualidad, una persona cuenta con una gran variedad de rasgos biométricos, susceptibles todos ellos para ser tratados, con diferentes técnicas y sistemas biométricos, para su identificación y autenticación.

2.2. ¿Qué es la biometría?

Todas estas mejoras, entre otras muchas, hicieron que el sistema de identificación de un usuario fuese cada vez más seguro, pero aún seguían apareciendo problemas en el proceso de Autenticación. En este contexto, y con el objetivo y la necesidad de identificar unívocamente a una persona, fue entonces cuando apareció la biometría. En este tercer paso, pasamos de “algo que sé” y “algo que tengo” a “algo que soy”.

La autenticación biométrica es el reconocimiento inequívoco de personas basado en un o más parámetros de comportamiento o rasgos físicos. Algunos de esos comportamientos pueden ser la forma de caminar, la firma manuscrita, el reconocimiento de voz y entre los rasgos físicos están la huella dactilar, la retina, el iris, la forma de la mano o las venas de la mano, la sangre, el ADN o la orina.

La principal ventaja del uso de la biometría para autentificar personas es que no hace falta llevar nada. Es decir, una persona podría autentificarse sin estar en posesión de un móvil o una tarjeta. Otra gran ventaja es que no hace falta tener capacidad para recordar multitud de contraseñas enormes para acceder a los sistemas o aplicaciones. Los datos biométricos no se pueden olvidar ni se pueden perder, ni robar, ni tampoco falsificar.

La autenticación por biometría puede usarse como complemento a la tradicional identificación de usuario por medio de login y contraseña, como aumento de capa de seguridad, doble factor, o puede usarse como único método

de autenticación al sistema o aplicación. En el primer caso, la identificación de usuario es mediante un login y la autenticación mediante una contraseña y como valor añadido, un segundo factor que sería la autenticación mediante biometría. En el segundo caso, tanto la identificación como la autenticación se realizan con biometría.

La identificación biométrica trata de identificar a una persona, ¿Quién es?

La autenticación biométrica es el proceso para verificar la identidad de una persona, es decir, que realmente una persona es quien dice ser.

Aunque la biometría se presente como una alternativa para la seguridad en los sistemas de autenticación, debemos tener en cuenta que existen tasas de errores, es decir, no existe la seguridad al 100%.

Cuando se decide el uso de biometría se debe de tener en cuenta el rendimiento de una medida biométrica elegida. Este rendimiento depende de la tasa de falso positivo, de la tasa de falso negativo y de la tasa de fallo de aislamiento.

Un sistema biométrico debe tener la capacidad de reconocer, medir, comparar y transmitir una característica o rasgo único de una persona y todo ello con la mayor precisión y fiabilidad. Por tanto, para acercarnos lo máximo posible a un 100%, debemos elegir un sistema biométrico que disponga de un hardware y un software lo más preciso posible en concordancia con el uso de una adecuada característica o rasgo biométrico. En la mayoría de los casos no es posible obtener este tipo de sistemas biométricos debido al alto coste económico. En consecuencia, debemos de tener siempre presente un umbral de error y/o tolerancia que se acerca lo máximo posible al 0%.

Al igual que ocurre con los sistemas biométrico, dos muestras de un mismo rasgo biológico no son exactamente iguales debido a imperfecciones, a factores ambientales, a la interacción de la persona con el sensor o depende de la calidad del sensor, como hemos detallado anteriormente.

Por tanto, cuando se realiza la comparativa del sistema biométrico se emite una puntuación que cuantifica la semejanza entre las dos muestras capturadas. A mayor puntuación mayor semejanza. La decisión se mide por un umbral, es decir, si la puntuación es mayor al umbral se acepta (las 2 muestras son de la misma persona) y si es menor se rechaza (muestras de diferentes personas).

A continuación, se muestra en la ilustración 2.1 y en la ilustración 2.2, las distribuciones de usuarios válidas y errores y los errores FA y FR según el umbral de similitud.

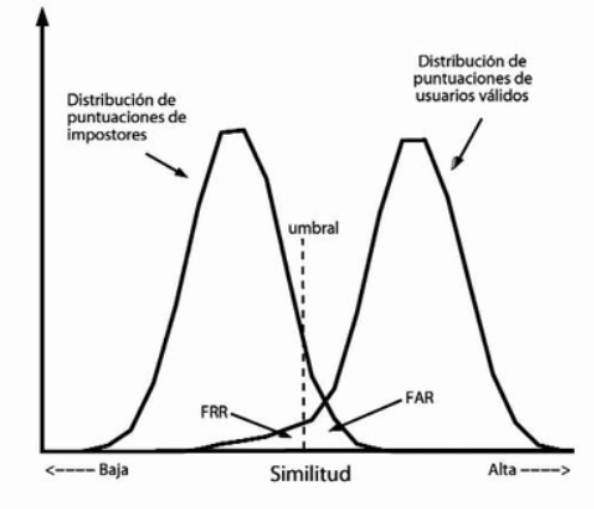


Ilustración 2.1: Distribuciones de usuarios válidos e impositores

Fuente: https://www.researchgate.net/publication/280722075_Seguridad_Biometrica

ilustración 2.2: Errores FA y FR en función del umbral de similitud

Fuente: https://www.researchgate.net/publication/280722075_Seguridad_Biometrica

Tasa de falsos positivos, TFP, son muestras falsamente asignadas a una persona a la que no pertenecen.

Tasa de falsos negativos, TFN, son muestras falsamente rechazadas como pertenecientes a una persona a la que sí pertenecen.

Tasa de Falsa Aceptación (FAR), veces que se acepta un intruso en el sistema

Tasa de Falso Rechazo (FRR), veces que se rechaza a una persona autentica del sistema.

Tasa de Igual Error (EER), valor donde FAR=FRR.

Todo esto se debe de tener en cuenta a la hora de diseñar un sistema de reconocimiento automático por biometría, además de asumir unos compromisos que dependan del coste y de la seguridad. Si elegimos un punto de trabajo extremo donde FRR=0 % y FAR=100 %, tenemos un sistema muy barato, pero totalmente inseguro. Por contra, si elegimos FAR=0% Biometría y Seguridad 26 y FRR=100%, el sistema no acepta a nadie y es necesario que todos los accesos sean comprobados por operarios manuales. Por tanto, la FRR puede usarse como definición del coste de un sistema:

Coste = FRR

Cuanto mayor sea la FRR, mayor es el coste de un sistema, puesto que más usuarios autorizados son incorrectamente rechazados, teniendo que invocar algún mecanismo de excepción, como que acuda un operario manual.

2.3. Clasificación de los sistemas biométricos

Una primera clasificación sería distinguir entre la medición de características biométricas físicas o corporales, a la que llamamos biometría estática y la medición de las características que dependen del comportamiento o conducta de una persona, a la que denominamos biometría dinámica.

Cada sistema de biométrico dependerá del uso para el que sea adaptado. Por tanto, aunque cada sistema se base en dispositivos con tecnologías diferentes, de forma genérica, un sistema biométrico se divide en 5 partes:

- Obtención de Datos
- Transmisión de Datos
- Procesamiento de la Señal
- Almacenamiento
- Decisión

La obtención de los datos, según el rasgo biométrico se recogerán con un dispositivo u otro, estos datos se trasmiten a un sistema digital informático donde se procesan las señales, aplicando unos filtros. Cuando obtenemos el vector de datos, se compara con una base de datos y se toma una decisión final sobre la verificación de la identidad de la persona. Si solo se está identificando y no verificando, no hay comparación en la base de datos, sino que solo se procesaría la información y cuando se obtiene el vector de datos se almacenaría en la base de datos asociado a una identidad. Podemos observarlo en la siguiente ilustración 2.3.

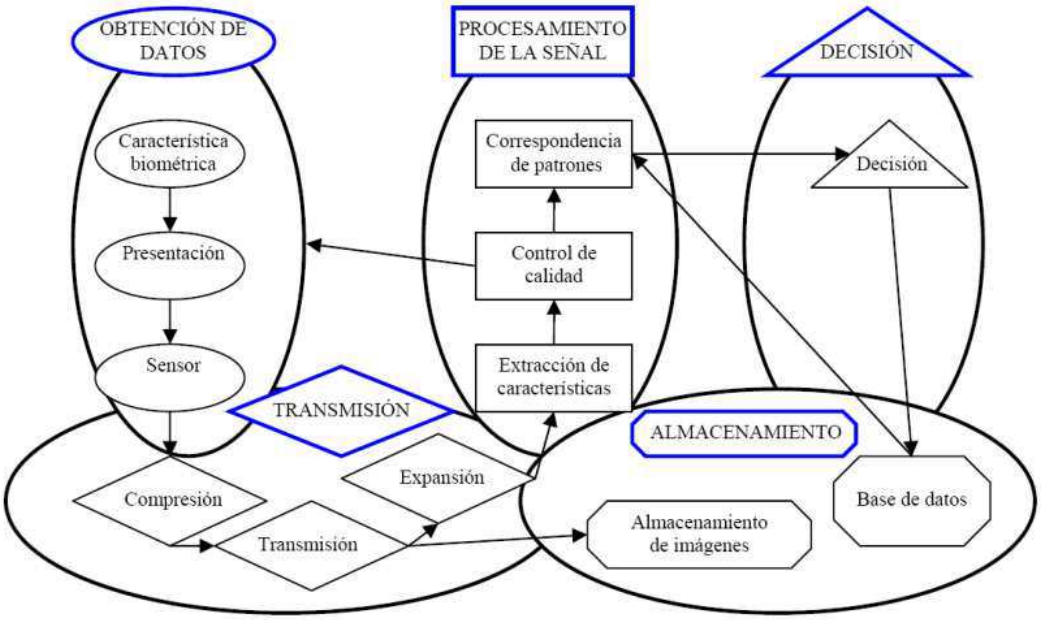


Ilustración 2.3: Diagrama de bloques de un sistema biométrico

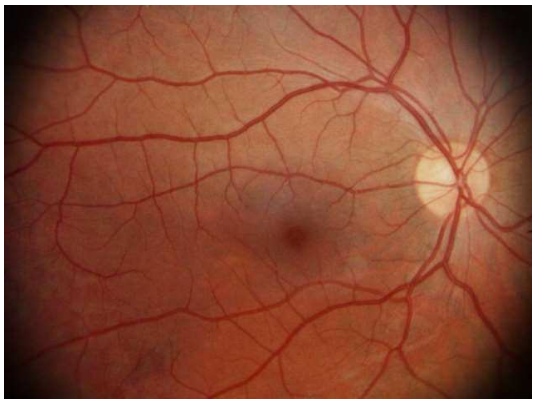
Fuente: http://oa.upm.es/20071/1/INVE_MEM_2012_143061.pdf

2.4. Algunas técnicas biométricas

La biometría, tal y como hemos explicado anteriormente, es una técnica para identificar a un usuario según unas características físicas o de comportamiento, en donde dicha identificación sea inequívoca. Para que la identificación sea lo más segura posible, es decir, intentando llegar al 100%, se deben escoger unos rasgos donde la fiabilidad y la seguridad no esté nunca comprometida. Podemos distinguir dos tipos de clasificaciones dependiendo de la técnica biométrica5. Una primera clasificación serían los rasgos estáticos, es decir, la característica nunca se altera o modifica, es la misma con el paso del tiempo, nunca cambia, como por ejemplo la retina, el iris, la huella dactilar, la forma de la cara y la mano, salvo algunas excepciones, como serían los retoques faciales estéticos. Por otro lado, están los rasgos dinámicos o de comportamiento. Éstos pueden sufrir alguna modificación con el paso del tiempo. Es decir, la forma de firmar, la forma de caminar, la voz, la manera de coger el móvil, no siempre son iguales, pueden variar dependiendo de estado del usuario. A continuación, se detallan los distintos tipos de rasgos de los usuarios.

2.4.1. Rasgos Estáticos

Retina: Forma parte del ojo, y se encuentra detrás del iris y de la pupila. La retina transforma la luz que entra por el ojo en impulsos eléctricos que se enviarán al cerebro a través del nervio óptico, para finalmente obtener las imágenes que vemos. La característica más importante de la retina son los vasos sanguíneos que la atraviesan.



[5] http://sedici.unlp.edu.ar/handle/10915/77053

Ilustración 2.4: Imagen de una retina

Fuente: https://biometrics-on.com/reconocimiento-biometrico-a-traves-de-retina/

Los dispositivos de reconocimiento por retina cuentan con una luz infrarroja que permite iluminar el fondo del ojo para capturar la imagen de la retina. Este paso es el más tedioso, ya que es imprescindible que la persona permanezca totalmente quieta y con el ojo lo más próximo posible al dispositivo. Una vez captura la imagen, se procesa aplicando unos filtros para extraer la zona de interés y se transforma mediante algoritmos. La mayoría de los algoritmos utilizan el proceso de esqueletización, que no es más que simplificación de la red vascular de capilares con una transformación a líneas de grosor de 1 píxel.

Iris: Es uno de los rasgos biométricos más seguros con una alta fiabilidad. El iris es una membrana de forma circular, formada por minúsculos músculos orbiculares y se encarga de regular el tamaño de la pupila, controlando la cantidad de luz que entra en el ojo. El iris es un rasgo único e inequívoco y es invariable a lo largo de la vida. Los iris de nuestros ojos son diferentes. Para el uso de sistemas de reconocimiento basado en iris, se deben usar imágenes de muy alta resolución, lo que encarece mucho el sistema.

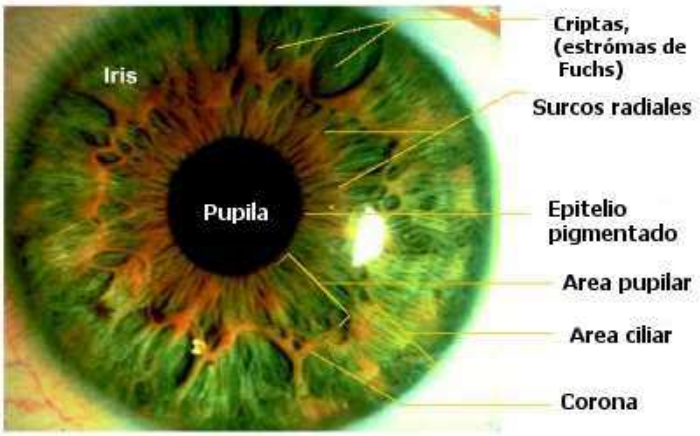


Ilustración 2.5: Características del Iris

Fuente: https://www.incibe-cert.es/blog/problematica-biometria-autenticacion

El procedimiento consta de una captura de imagen de alta resolución, se almacena la imagen mediante un algoritmo conocido por Daugman [13], donde se obtiene un único IrisCode con un tamaño aproximado de 256Kb.

Posteriormente se compara con una base de datos de patrones para identificar su identidad.

Facial: El reconocimiento facial identifica a personas mediante la medición de la forma y estructura de la cara. Al contrario de lo que ocurre con el iris o la retina, el reconocimiento facial no es un rasgo inalterable para toda la vida, ya que depende de factores como el envejecimiento, cosmética, cirugía plástica, consumo de alcohol y/o drogas, etc. El funcionamiento de este proceso de reconocimiento es muy simple: se captura la imagen, se alinea el rostro, se extraen las características faciales, se aplica un algoritmo y se obtiene un vector característico que será comparado en una base de datos para la identificación de esa persona.

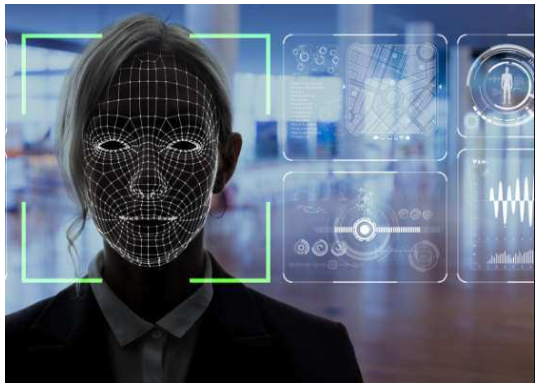


Ilustración 2.6: Reconocimiento facial.

Fuente: https://www.pandasecurity.com/spain/mediacenter/mobile-news/reconocimiento-facial-se-convierten-en-debate-viral/

Este tipo de reconocimiento presenta muchos problemas: inconvenientes de la iluminación, alineación de la pose del rostro, suplantación mediante una fotografía en sistemas 2D, etc.

Geometría de la Mano: A diferencia de otros rasgos biométricos, la mano de una persona no es única. La mano está compuesta por 27 huesos, 36 articulaciones y 39 músculos y la combinación de estas características hace posible identificar a una persona.

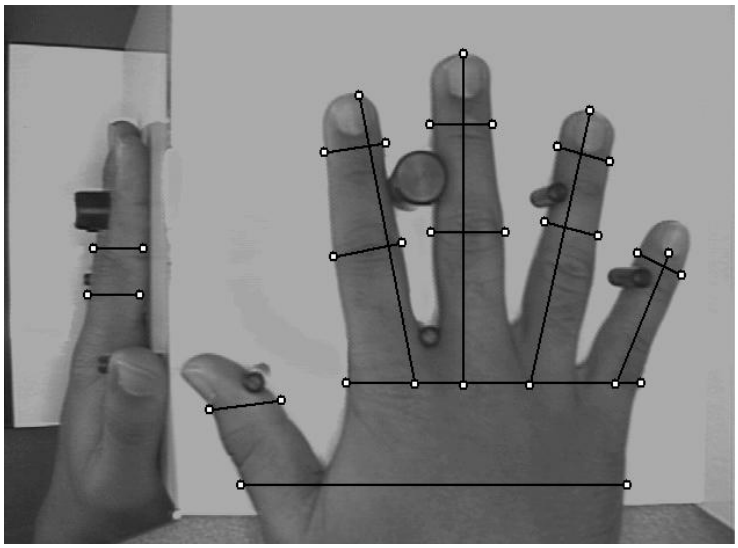


Ilustración 2.7: Geometría de mano

Fuente: https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node120.html

El procedimiento es sencillo. Se toman tres muestras de la mano, capturando imágenes laterales y superior para extraer características como el grosor, longitud, área, etc. Las imágenes obtenidas se procesan a una resolución de 640x480 pixeles y con 256 colores. Con el promedio de esas imágenes, se forma un patrón con un tamaño de 9 bytes el cual será comparado en una base de datos para identificar a una persona.

Entre sus características destacamos la rapidez del proceso, independencia de factores ambientales como ruido o luz, bajo coste económico y fácil de utilizar. Por el contrario, su tasa de fiabilidad es menor que con otros rasgos biométricos, es susceptible a cambios físicos de la mano, depende de la cooperación del usuario, no es recomendable para grupo elevado de personas, etc.

Huella dactilar: Es la característica más usada en biometría. Es la impresión que deja el contacto de las crestas capilares de las yemas de los dedos de la mano con una superficie, según la Rae[6]. La huella dactilar no es clara, por ese motivo no hay dos huellas dactilares iguales. Está formada por crestas papilares que a su vez forman unos relieves epidérmicos y el espacio

[6] https://dpej.rae.es/lema/huella-dactilar

que se forma entre ellos se llaman surcos interpapilares o valles. Los dibujos o figuras que forman las crestas papilares reciben el nombre de dactilogramas.

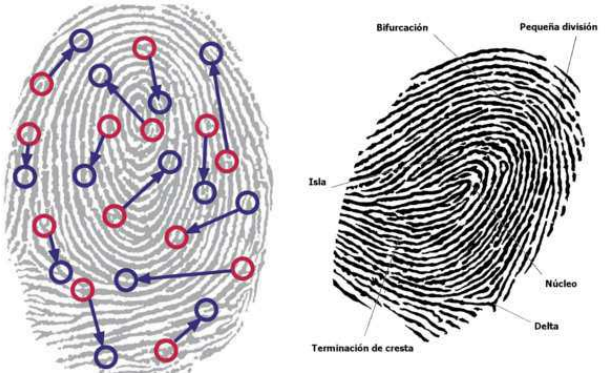


Ilustración 2.8: Características de una huella dactilar

Fuente: https://www.incibe-cert.es/blog/problematica-biometria-autenticacion

Su reconocimiento puede estar basado en minucias, donde se identifican las formas de la huella y su ubicación, o puede estar basado en correlación, donde se comprueba la huella dactilar completa.

Un ejemplo de ello es la marca HITACHI, que ha desarrollado un lector de venas de dedos que identifica inequívocamente a personas. La herramienta se llama VeinID Five[7] y ya está implantado en varios bancos del Reino Unido.

2.4.2. Rasgos Dinámicos

Voz: Los pulmones producen un flujo de aire provocando el choque entre las 2 cuerdas vocales, que, junto al tracto vocal, emiten un sonido rígido compuesto por un tono y un timbre.

Un sistema de reconocimiento por voz capta la señal de voz que emite una persona, la procesa en un sistema informático y posteriormente la compara para obtener su identificación. Es un sistema fácil y rápido, pero, por el contrario, tiene un gran inconveniente que es su facilidad para grabar y reproducir sonidos con la intención de usurpar la identidad.

[7] https://digitalsecurity.hitachi.eu/

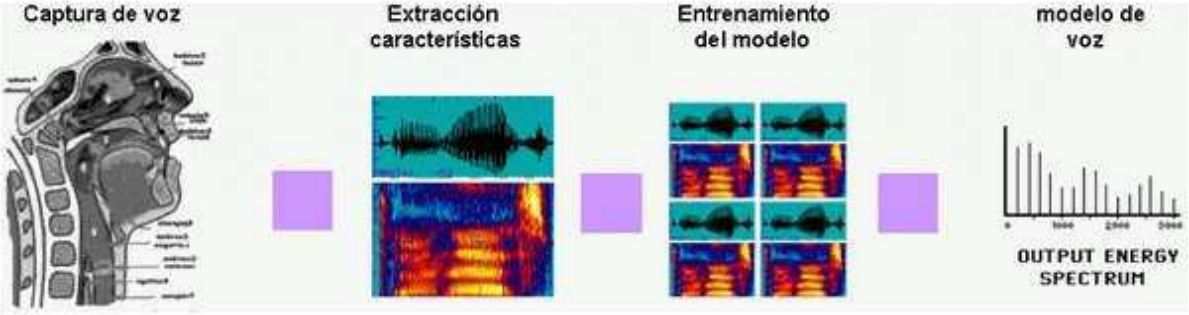


Ilustración 2.9: Proceso de reconocimiento de voz

Fuente: https://www.um.es/web/dis/

El sistema de reconocimiento por voz está en auge por el despliegue en la actualidad del internet de las cosas, los famosos dispositivos IoT.

Firma: Se compone de unos trazos y unos rasgos. La firma manuscrita de una persona siempre sufre ligeras variaciones, ya que depende del movimiento al firmar, de las condiciones físicas de la mano, del útil que estemos usando para realizar la firma (lápiz, pluma, bolígrafo, etc.), etc.

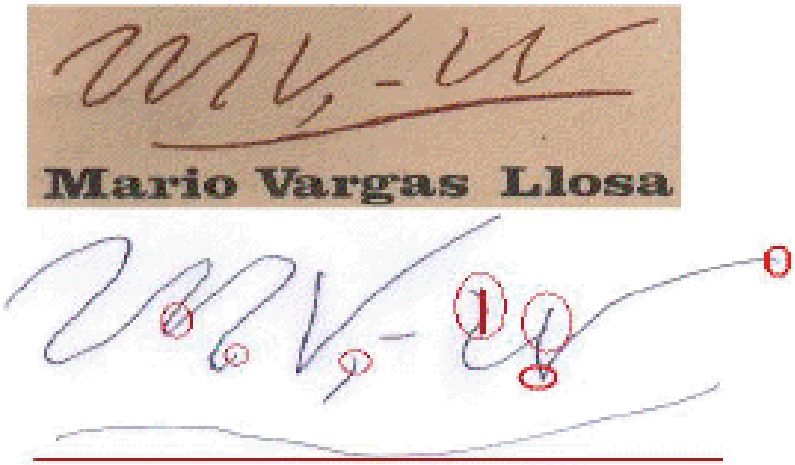


Ilustración 2.10: Puntos para analizar de una firma

Fuente: https://sites.google.com/a/ci2s.com.ar/wiki/technics/fundamentos-grafologicos-de-la-firma-manuscrita

Existen dos modalidades de reconocimiento. Estático u Off-Line, donde la firma se lleva a cabo sobre un papel y posteriormente, mediante escáner o cámara de fotos, se analiza en un sistema informático. Dinámico u On-Line, donde la persona realiza el acto de firma sobre un sistema digital (Tablet, PDA, etc.) Con esta técnica se obtiene la firma a tiempo real, pudiendo el sistema,

captar otras características importantes como la velocidad, la aceleración, la presión, el tiempo, la inclinación y las coordenadas espaciales (x, y).

La principal desventaja que posee es su alto porcentaje de falsificación.

Caminar: es una característica del comportamiento de una persona, por lo que no es siempre igual. Depende de factores como la salud de la persona, la superficie por la que se camina, el calzado utilizado, etc. Todo ello dificulta su fiabilidad y aumenta la posibilidad de posibles imitaciones. Como consecuencia, por sí solo, no es un rasgo biométrico muy usado para identificación de personas. Aún está en estudio y desarrollo.

Authcode: llamado también Código de autorización, código de autenticación o código de transferencia. Es un código creado por un registrador de un dominio indicado para identificar al titular de un dominio, a su propietario. Es obligatorio para la trasferencia de dominios de un registrador o titular a otro.

Historial de aplicaciones: Los terminales smartphone, tabletas, relojes inteligentes o cualquiera de los dispositivos que usen y/o tengan instaladas aplicaciones almacenan un historial del uso que se hace de dichas aplicaciones. Es decir, cuáles son las más usadas, que tiempo de uso se hace de cada una de ellas, en qué horarios son usadas, si están ejecutándose en segundo plano o no, etc. Por tanto, las aplicaciones facilitan mucha información del comportamiento que realiza el usuario sobre ellas.

Según el estudio Global Mobile Consumer Survey 2017[8], elaborado por Deloitte, los españoles tienen una media de 16 aplicaciones instaladas en sus smartphones, sólo el 41% de los usuarios limita su uso, el 69% prefieren conexiones WI-FI para navegar y, aun así, más del 50% agotan la cantidad de datos disponibles mensualmente.

Ergonomía: Hay varias maneras de coger un terminal móvil, con una o dos manos y, sobre todo, los dedos más usados para manejar un smartphone son

[8] https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia-media-telecomunicaciones/Deloitte-ES-TMT-Consumo-Movil-2017.pdf

los dedos índices y pulgar. La forma de coger un smartphone determina que zonas de la pantalla son las más usadas, que trae como consecuencia, donde están ubicadas las aplicaciones más usadas por el usuario.

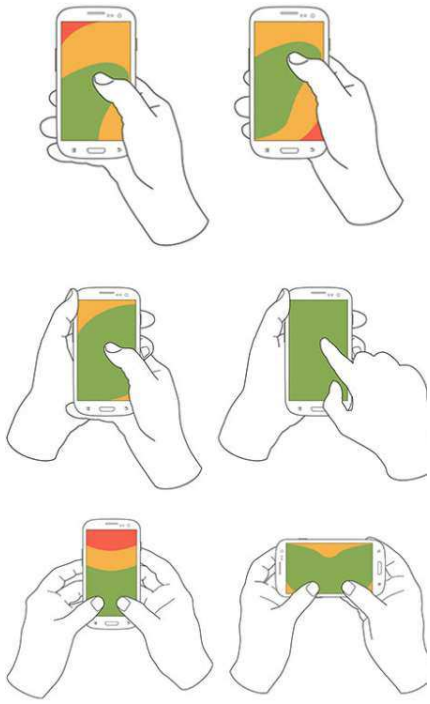


Ilustración 2.11: Formas de coger un móvil

Fuente: http://www.rubenalcaraz.es/pinakes/diseno-web/webs-aplicaciones-moviles-punto-vista-ux/

3. PROPUESTA

Debido al problema que hemos detectado y explicado anteriormente, sobre la complejidad de la identificación de los usuarios mediante el uso de biometría, si hacemos una búsqueda en el mercado de cómo realizar dicha identificación con parámetros biométricos, nos damos cuenta que, según los parámetros o características que escojamos para la identificación, como por ejemplo el iris o la retina, puede resultar tedioso además de costoso y a la vez de poco eficaz9, realizar dicha identificación de forma segura. Sin embargo, si escogemos otras características, como por ejemplo la huella dactilar o reconocimiento facial y los combinamos con otros métodos no biométricos, podemos obtener una identificación de usuario también muy eficaz y mucho menos costosa. Por tanto, a continuación, se propone realizar una mejora de dicha identificación de usuarios usando parámetros biológicos que llevan asociados a su vez algún sensor biométrico instalado en un terminal ya sea móvil, tableta o smartwatch.

Este Trabajo Fin de Máster (TFM), presenta una propuesta de estudio de mejora en la Identificación de los Usuarios mediante tres escenarios diferentes según su nivel de complejidad, usando sensores de magnitudes físicas capaces de identificar rasgos biométricos del usuario que los usa.

En concreto, un primer escenario, donde se pone en valor la identificación de usuarios usando el sensor GPS. Un segundo escenario, con un nivel más de complejidad, en el cual, se estudia combinar el sensor GPS con el acelerómetro. Un tercer escenario, donde se añade el histórico de uso de las aplicaciones instaladas en el terminal móvil, al escenario que ya teníamos anteriormente, aumentando así la complejidad hasta un nivel superior.

A través de esta propuesta, se pretende que un usuario pueda identificarse, de la manera más rápida y segura, utilizando “algo que soy”, es decir, un rasgo biométrico que del que nunca se pueda desprender.

[9] https://es.linkedin.com/pulse/biometr%C3%ADa-de-iris-vs-retina-estudio-tecnol%C3%B3gico-luis-alberto-nieto

Antes de continuar, explicamos brevemente que es un sensor. Un sensor es un dispositivo capaz de dar respuesta eléctrica a estímulos físicos, es decir, detectar acciones externas y responder. Son capaces de medir magnitudes físicas como temperatura, humedad, luz, longitud, etc., o también son capaces de medir magnitudes químicas como por ejemplo el nivel de azúcar en sangre, el nivel de cloro en una piscina, o el nivel de oxígeno en una habitación.

Un terminal móvil está compuesto por muchísimos sensores diminutos que habitan entre sí en su interior. Sensor de humedad, de temperatura, cámara, infrarrojos, acelerómetro, GPS, giroscopio, magnetómetro, micrófono, etc.

3.1. Identificación mediante GPS

En este primer escenario, se intenta mejorar la identificación de usuarios mediante el uso del sensor GPS instalado en los terminales móviles, Tabletas o smartwatches. Este sensor puede ser usado para geolocalización y para georreferenciación, aunque en esta propuesta sólo se va a abordar la geolocalización. La geolocalización es la capacidad de conocer la posición geográfica (en coordenadas) o ubicación de la persona u objeto que está haciendo uso de ella. Por tanto, mediante la geolocalización, se obtendrán los datos de ubicación de un usuario con una precisión de centímetros, conllevando a obtener un registro horario del movimiento y los desplazamientos de dicho usuario: posición en el tiempo, descripción de itinerario geográfico y tiempo transcurrido, etc. Es decir, entran en juego directamente las magnitudes de “tiempo” y “lugar”.

3.1.1. GPS: Global Positioning System

El GPS, *Global Positioning System*, es un sistema de Posicionamiento Global que permite determinar la posición exacta, con una cierta precisión de hasta unos centímetros. Nació en el Departamento de Defensa de los Estados Unidos con el nombre de NAVSTAR GPS y es propiedad de la Fuerza Espacial de los EE. UU. Actualmente sólo hay dos sistemas de posicionamiento por satélite, el mencionado NAVSTAR GPS de EE. UU. y GLONASS propiedad de Rusia, aunque la Unión Europea y China también están desarrollando un prototipo.

Mediante la colaboración de una red de 24 satélites (4 x 6 orbitas) que orbitan alrededor de la tierra, el sistema de posicionamiento triangula nuestra posición con un mínimo de 3 satélites, aunque normalmente se utilizan 4, permitiendo obtener una posición con una ubicación en 3 dimensiones: latitud, longitud y altitud. Se puede añadir la dimensión del tiempo para obtener una identificación más precisa con 4 dimensiones. La precisión de un GPS dependerá del número de satélites visibles en el momento y posición determinados. Aplicaciones móviles como Google Maps usa este método de geolocalización.

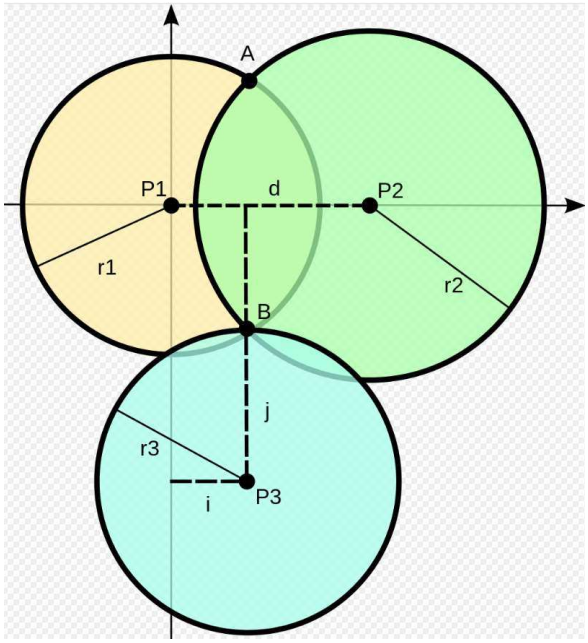


Ilustración 3.1: Triangulación de 3 satélites

Fuente: https://es.wikipedia.org/wiki/Trilateraci%C3%B3n#/media/Archivo:Trilateration.svg

Actualmente, la mayoría de los smartphones que existen en el mercado, cuentan con sensores GPS, que calculan su posicionamiento en tiempo real. El GPS no consume datos de nuestro terminal, pero si consume un alto porcentaje de batería, debido al continuo envío-recepción de información de los satélites. Como consecuencia de ello, apareció el sistema A-GPS (*Assisted Global Positioning System),* presente en la gran mayoría de smartphone del mercado, y no es más que un sistema de asistencia al GPS convencional. Es decir, combina el sistema de posicionamiento global mediante recepción de datos de los

satélites, con información que recogen de las antenas de telefonía móvil y antenas wifi a la que se conecta el smartphone (GPS, GSM y WIFI / WPS). En ubicaciones abiertas, el GPS tiene mayor precisión y menor costo de datos, pero en ubicaciones donde existen obstáculos de comunicación, grandes edificaciones, zonas urbanas, incluso climatología adversa, la solución A-GPS mejora la precisión del GPS del smartphone y reduce el consumo de batería y datos, ya que puede llegar a usarse mediante wifi o conexión pc para evitar conexión por móvil.

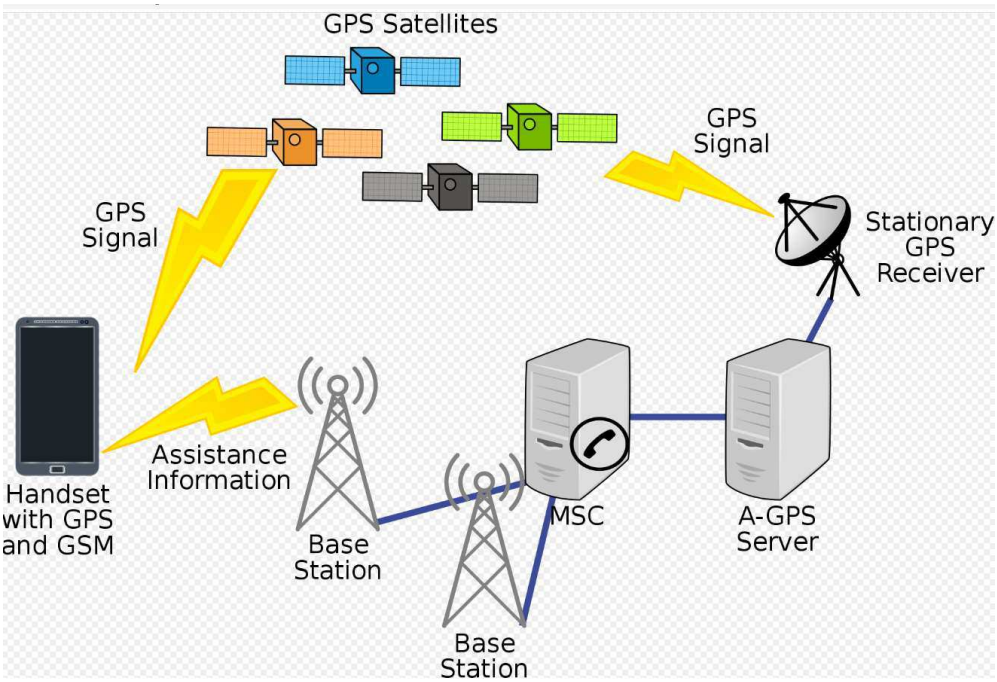


Ilustración 3.2: A-GPS

Fuente: https://en.wikipedia.org/wiki/Assisted_GPS

Se puede decir que la geolocalización es un rasgo biométrico de comportamiento. En ámbitos como en la banca online o en la identificación para accesos físicos, juega un papel muy importante, ya que, permite conocer la posición de un terminal a tiempo real y, por tanto, se pueden crear zonas o regiones de acceso habilitado o, por el contrario, zonas de acceso restringido.

Un ejemplo de ello se puede ver en la compañía VISA, que ha presentado Mobile Location Confirmation o Confirmación de Localización Móvil[10],. Es un sistema de seguridad mediante geolocalización que identificará si el titular de la

[10] https://hipertextual.com/2016/09/seguridad-movil-geolocalizacion

tarjeta de crédito con la que se está realizando el pago está localizado en las proximidades de local donde se está realizando el pago con dicha tarjeta Visa.

Otros ejemplos del uso de geolocalización serían la aprobación de operaciones realizadas con un móvil dentro de una zona habilitada para ello, como registro en aplicaciones, apertura de puertas físicas, fichajes en oficinas. Denegar operaciones realizadas en zonas restringidas, transacciones bancarias, accesos a bases de datos o fichajes erróneos.

Por tanto, podemos decir que la geolocalización aumenta seguridad, aumenta la robustez en sistemas de autenticación, evita phishing o transacciones económicas como blanqueos de capitales.

3.1.2. Amenazas y Vulnerabilidades de la Geolocalización

El GPS permite la localización física de cualquier usuario en cualquier lugar del mundo en tiempo real. Este acto posee consecuencias directas en la privacidad del usuario, ya que se detalla su ubicación frente a cualquier posible atacante.

Las aplicaciones sociales que existen en la actualidad están basadas en localización, obtienen las coordenadas geográficas de la ubicación del usuario, las procesan y posteriormente las analizan para ofrecer sus servicios. Todo ello conlleva un grave riesgo para la privacidad del usuario. Obtención de publicidad personalizada en función de la ubicación, analizar nuestro comportamiento con usuario para mejorar “experiencias de uso” de aplicaciones, ser partícipes de estudios para mejor de sistemas operativos o nuevas tecnologías.

3.2. Identificación mediante GPS y Acelerómetro

3.2.1. Acelerómetro

Un acelerómetro es un dispositivo electromecánico, fabricado con silicio, que se usa para medir las fuerzas de aceleración en los objetos donde va acoplado. Mide las fuerzas gravitatorias en los ejes (X, Y, Z) con el circuito interno de un chip. La aceleración es la fuerza que se le aplica a una masa y existen dos tipos de fuerzas: la estática, que es la fuerza de la gravedad y como

su nombre indica, es una fuerza constante; y las fuerzas dinámicas, que son los movimientos o vibraciones que se realizan.

Para entender la aceleración se debe partir de la *segunda Ley de Newton*, un principio físico donde F = m * a. Por tanto, la aceleración es proporcional a la fuerza que actúa sobre ella e inversamente proporcional a su masa. Hay que tener en cuenta que, tanto la aceleración como las fuerzas, poseen magnitudes y direcciones, es decir, son cantidades vectoriales.

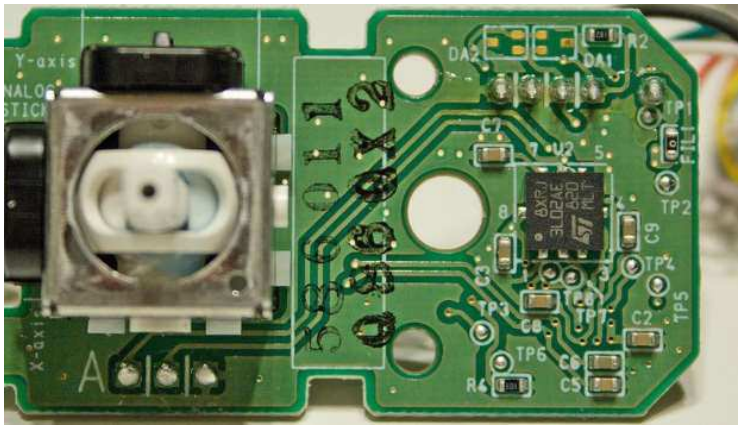


Ilustración 3.3: Acelerómetro de un terminal móvil

Fuente: https://www.eldiario.es/hojaderouter/tecnologia/acelerometro-funciones-giroscopio-gps-interior-magnetometro-sensor-sensor-de-humedad-sensor-de-temperatura-telefono-movil_1_4793670.html

3.2.2. Funcionamiento del acelerómetro en un terminal móvil

El acelerómetro basa su movimiento dependiendo de un condensador. Dos placas metálicas, una fija y otra móvil, en posición paralela, componen el condensador. Cuando se produce el movimiento en un terminal, la placa que no está fija, la móvil, varía su posición, se desplaza, aumentando o reduciendo su distancia respecto a la placa fija, por tanto, la capacidad del condensador cambia. Además del condensador, también hay un material dieléctrico, que suele ser un papel, que almacena la energía que llega de las dos placas del condensador.

Finalmente, el sensor calcula la cantidad de carga eléctrica que enviará al chip para que la procese y calcule la aceleración producida, la cual se tendrá en cuenta para inmediatamente realizar una acción en el sistema.

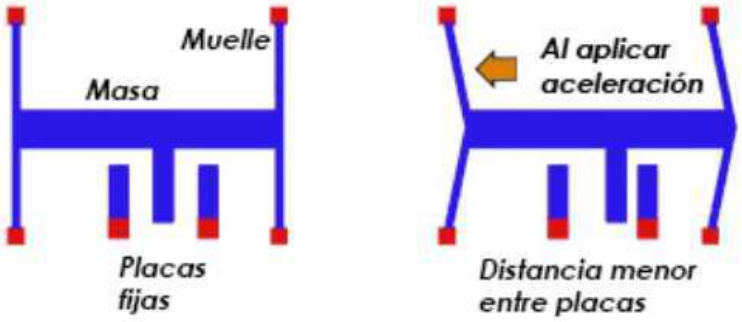


Ilustración 3.4: Fundamento físico de un acelerómetro capacitivo

Fuente: https://atomosybits.com/la-fisica-tras-el-acelerometro/

El acelerómetro es el culpable de detectar la orientación y rotar la interfaz en la pantalla de un terminal móvil. Actualmente se pueden encontrar acelerómetros en smartphones, Laptops o video consolas, como es el caso de la Nintendo Wii.

3.2.3. Vulnerabilidades de un acelerómetro

Según un estudio realizado hace unos años en la universidad de Michigan y la universidad de Carolina del Sur, el equipo del profesor Kevin Fu[11], se descubrió que la música podría engañar a los acelerómetros[12]. Cuando se escucha música cerca de un acelerómetro, el sonido emite unas ondas acústicas que vibran por la carga, y como consecuencia de ello podrían hacer vibrar las placas del condensador emitiendo una señal eléctrica. Se estaría engañando al acelerómetro haciéndolo creer que está en movimiento cuando no es así.

Accelprint[13] se descubrió hace unos años. Es un ataque al acelerómetro de los terminales móvil o Tablet, el cual permite rastrear dispositivos sin necesidad del permiso del usuario. Está basado en las imperfecciones que poseen los sensores en su fabricación, descubriendo que cada sensor responde casi de forma univoca a estímulos iguales, pudiendo así diferenciar mediante reconocimiento de patrones. Esa respuesta unívoca sería su "cookie electrónica". Si se logra comprometer el dispositivo se tendría acceso al

[11] https://nakedsecurity.sophos.com/es/2017/03/22/soundwaves-used-to-produce-fake-data-from-accelerometers/
[12] https://spqrlab1.github.io/papers/trippel-IEEE-oaklawn-walnut-2017.pdf
[13] https://www.ndss-symposium.org/ndss2014/programme/accelprint-imperfections-accelerometers-make-smartphones-trackable/

acelerómetro y generar su identificación única “token” mediante la API oficial. Así, se podría controlar la ubicación e información privada.

3.2.4. GPS + Acelerómetro

Si al simple hecho de realizar una autenticación como usuario, unimos ahora dos factores más para realizar esa autenticación, el nivel de seguridad en el proceso aumenta considerablemente, aunque nunca es 100% seguro.

Pues bien, si unimos el sensor de GPS y el sensor de acelerómetro de un dispositivo móvil, su identificación o, por el contrario, el intento de vulneración en el proceso de autenticación de un usuario es ahora más tedioso, ya que han de cumplirse dos requisitos biométricos físicos.

Para completar el proceso de autenticación deben cumplirse los requisitos de los dos factores de autorización. Por una parte, la posición del GPS del terminal debe ser la correcta, es decir, el terminal debe de estar ubicado dentro de la zona permitida para dicha autorización y además ahora sumamos que el movimiento del móvil también debe de cumplir unos requisitos predefinidos, como por ejemplo una orientación autorizada. Si el terminal reúne en ese momento las condiciones predefinidas, entonces se llevará a cabo dicha autorización del usuario y ésta será favorable. De lo contrario, no será factible la autenticación.

3.3. Identificación mediante GPS y Acelerómetro y uso de APPS

3.3.1. Historial de uso de las aplicaciones

Hoy en día podemos comprobar el uso de las aplicaciones que tienen instaladas los dispositivos móviles o tabletas. Hay dos maneras de obtener dicha información: mediante el propio sistema operativo del dispositivo o mediante el uso de aplicaciones externas.

Lo primero que se debe conocer es donde está ubicado el historial de uso en nuestros dispositivos.

En un sistema operativo Android se deberá seguir los siguientes pasos en ajustes -> batería -> Estadísticas del uso de la batería (uso de la batería)

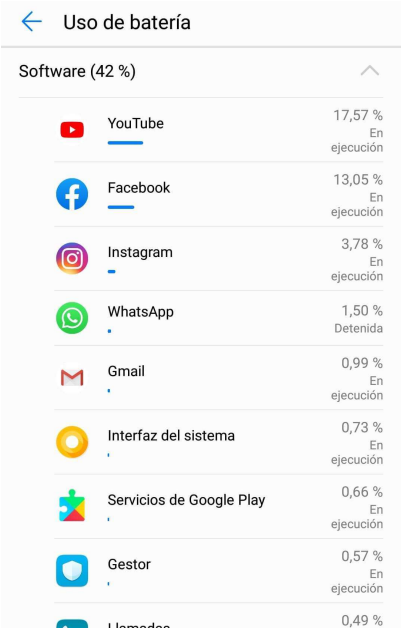


Ilustración 3.5: Historial de uso de aplicaciones en un terminal Android

En un sistema iOS, podrá encontrarlo en ajustes -> Tiempo de uso

Ilustración 3.6: Historial de uso de aplicaciones en un terminal iOS

Con este servicio integrado en el sistema operativo, se podrá consultar a tiempo real, el uso que se está realizando en cada aplicación. Es importante para determinar si alguna aplicación se está usando en segundo plano sin tener constancia de ello el usuario.

3.3.2. Identificación mediante uso de las Apps

Cada dispositivo móvil usa varios identificadores únicos para la interconexión con servicios y aplicaciones. El código IMEI, identifica un

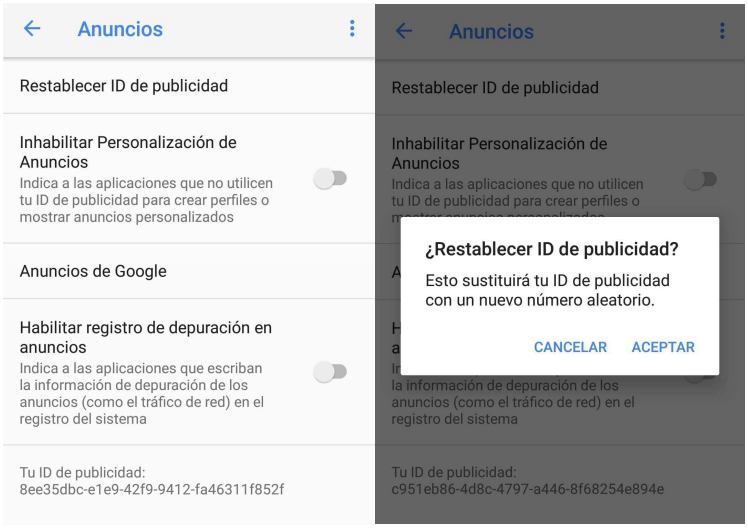
dispositivo y usarse para su bloqueo en caso de pérdida o robo. La dirección MAC, permite la interconexión, puede usarse para añadir en una lista los dispositivos permitidos o, por lo contrario, para restringir. El número de serie puede identificar a todos los dispositivos de un mismo lote de fabricación en caso de algún defecto. ID de Android, SSAID, sirve para gestionar licencias de aplicaciones. En teoría, estos identificadores pueden ser modificados. Bien con aplicaciones que existen para ello o haciendo rooting, lo cual hace vulnerable al dispositivo, pero, en algunos países se considera ilegal.

En 2013 Google lanzó el ID de publicidad[14]. Google Play asigna un ID a cada dispositivo móvil, la cual sólo se puede usar con fines comerciales y no prohíbe enlazarse con otro identificador del dispositivo, pero el usuario debe confirmar el consentimiento. Por desgracia, algunas de las aplicaciones que hay en la actualidad, enlazan los identificadores y no piden su previo consentimiento al usuario.

En el caso de Apple, toda la información incluida en el identificador de publicidad asignado a tu Apple ID se usa para determinar en qué segmentos se te incluye y en qué anuncios recibes.

Se puede restablecer cada vez que se quiera:

Ajustes -> Google -> Anuncios -> Restablecer ID de publicidad



[14] https://support.google.com/admanager/answer/6274238?hl=es#

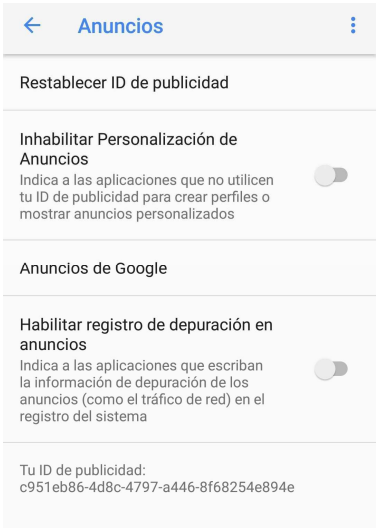


Ilustración 3.7: Modificación de ID de publicidad

Como puede observarse en las imágenes anteriores, el dispositivo móvil disponía de una ID de publicidad, y después de restablecer, esta ID de publicidad se ha modificado.

Como consecuencia, las redes publicitarias, mediante el ID de publicidad, pueden enviar publicidad a los dispositivos, identificando nuestros gustos o preferencias según las aplicaciones que utilicemos, o según los buscadores. Otra forma de identificar al usuario según sus preferencias.

Por otro lado, hay que tener presente que en los terminal smartphone hay instalada al menos una cuenta de correo electrónico. Pues bien, a través de dicha cuenta asociada en dicho terminal se pueden realizar varias comprobaciones:

- Ver y controlar la actividad que se realiza desde el terminal, es decir, búsquedas que se realizan, sitios web visitados, videos que se miran, lugares a los que vamos.
- Revisar el historial y las cookies en los navegadores.
- Revisar y borrar archivos.
- Compartir información de uso y diagnóstico.
- Visualizar y controlar la actividad de aplicaciones.
- Grabaciones de audio.
- Etc.

Si bien nos parecía tedioso el intento de vulnerabilidad de una identificación de un usuario con el uso de 2 MFA, localización por GPS y acelerómetro, ahora aumentamos hasta un tercer nivel la seguridad, añadiendo como tercera condición o tercer factor, el historial de uso de un dispositivo móvil. Por tanto, aumentamos la seguridad y se disminuye el riesgo de una suplantación o robo de identidad, sabiendo siempre, que el riesgo cero no existe.

3.3.3. GPS + Acelerómetro + Uso de las Apps

Como hemos detallado anteriormente, para que se produzca la autenticación mediante GPS + Acelerómetro, debe confluir dos factores, por un lado, que la posición del GPS del terminal sea la correcta y, por otro lado, que la orientación del smartphone también sea la definida en dicho proceso. Ahora bien, para nuestro escenario tercer escenario hemos elegido el historial de uso de las aplicaciones como tercer factor. Un uso correcto y definido. Por ejemplo, si se suele usar solo el navegador Chrome y nunca o casi nunca se usa el Firefox, pues si se intenta realizar la autenticación mediante ese navegador, el proceso de autenticación debe de fallar y lanzar aviso. Otro error de autenticación sería si se intentase la autenticación mediante una aplicación que nunca usamos. Si tenemos descargada una aplicación bancaria en nuestro terminal, pero revisando el historial de uso vemos que nunca se usa, entonces, si se intenta realizar el proceso de autenticación desde dicha aplicación, el proceso debe de fallar y lanzar una alarma o aviso.

Por tanto, en este tercer escenario, para que llegue a producirse correctamente el proceso de identificación del usuario que está haciendo uso del terminal, deben de concluir 3 factores: posición del GPS, orientación del smartphone y uso correcto de las aplicaciones previamente definidas.

4. PROTOTIPO

4.1. Desarrollo del prototipo

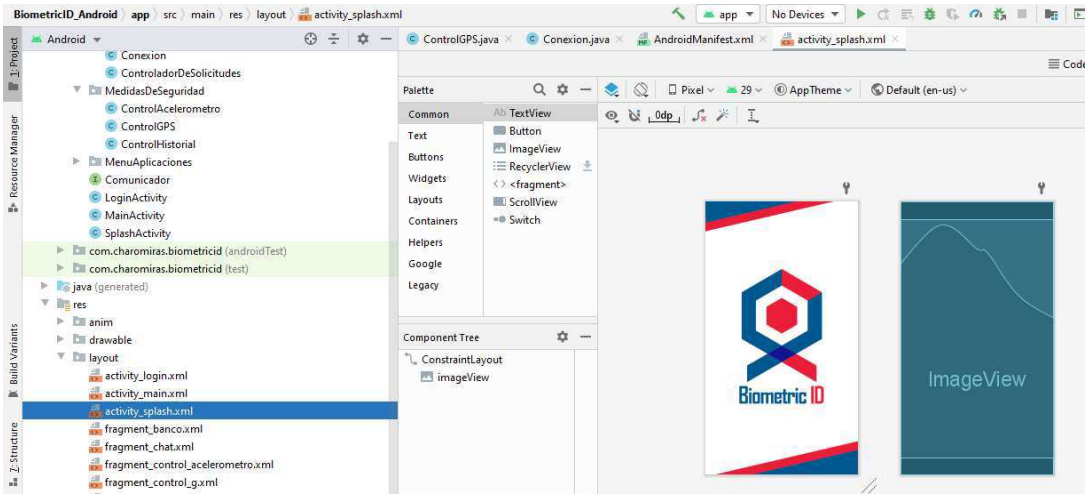
4.1.1. Introducción

El prototipo propuesto es una aplicación desarrollada en sistema operativo Android para terminales móviles y tablet, a la que he llamado BiometricID. La idea de escoger ese nombre, es debida, a la actividad para la que se desarrolla dicha aplicación, mejora de identificacion con biometría.

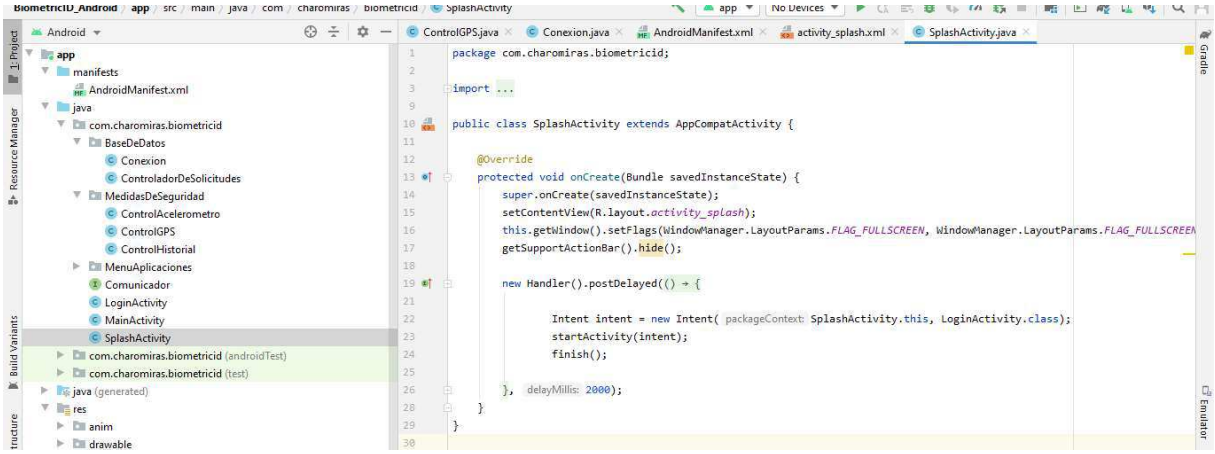
Es una aplicación desarrollada con el software Android Studio para Android. Se basa en el uso de tres activity[15]: SplashActivity[16], LoginActivity[17] y MainActivity[18].

```
android:theme="@style/AppTheme">
    <activity android:name=".MainActivity"></activity>
    <activity android:name=".LoginActivity"
        android:screenOrientation="portrait"/>
    <activity android:name=".SplashActivity"
        android:screenOrientation="portrait">
        <intent-filter>
```

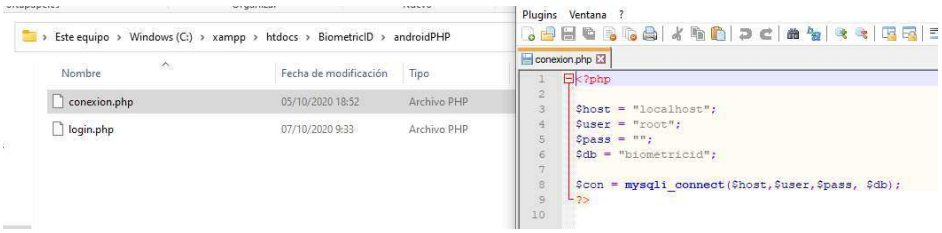
Por defecto, cuando se inicia la App está predeterminada SplashActivity, que es la pantalla de bienvenida.



[15] https://developer.android.com/guide/components/activities/intro-activities?hl=es
[16] https://developer.android.com/about/versions/12/features/splash-screen
[17] https://developer.android.com/codelabs/biometric-login#0
[18] https://developer.android.com/guide/topics/manifest/manifest-intro?hl=es-419



Esta actividad lo único que hace es abrir la pantalla de bienvenida que es el logotipo de la App, espera 2 segundos y seguidamente abre la pantalla de login. Para ello, se ha tenido que configurar previamente la URL para que conecte con el portal web y se realice correctamente la conexión a la base de datos.

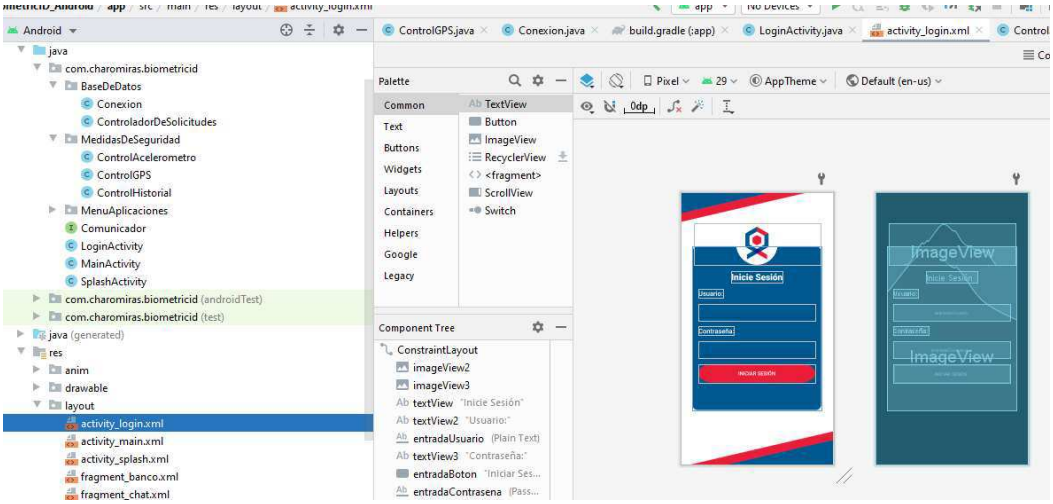


El controlador de solicitudes es una clase que se usa también para la realización de la conexión. Contiene dos dependencias, la dependencia ‘volley’, que es la encargada de realizar la conexión php con la base de datos y la dependencia ‘styleabletoast’, que son las ventanas pop-up que aparecerán con los mensajes en la aplicación, así se consigue darles estilo a esos mensajes.

```java
public class ControladorDeSolicitudes {
    private static ControladorDeSolicitudes mInstance;
    private RequestQueue mRequestQueue;
    private static Context mCtx;

    private ControladorDeSolicitudes(Context context) {
        mCtx = context;
        mRequestQueue = getRequestQueue();
    }

    public static synchronized ControladorDeSolicitudes getInstance(Context context) {
        if (mInstance == null) {
            mInstance = new ControladorDeSolicitudes(context);
        }
        return mInstance;
    }

    public RequestQueue getRequestQueue() {
        if (mRequestQueue == null) {
            mRequestQueue = Volley.newRequestQueue(mCtx.getApplicationContext());
        }
        return mRequestQueue;
    }

    public <T> void addToRequestQueue(Request<T> req) { getRequestQueue().add(req); }
}
```

```gradle
dependencies {
    implementation fileTree(dir: 'libs', include: ['*.jar'])
    implementation 'androidx.appcompat:appcompat:1.0.2'
    implementation 'androidx.constraintlayout:constraintlayout:1.1.3'
    implementation 'androidx.legacy:legacy-support-v4:1.0.0'
    testImplementation 'junit:junit:4.12'
    androidTestImplementation 'androidx.test.ext:junit:1.1.0'
    androidTestImplementation 'androidx.test.espresso:espresso-core:3.1.1'
    implementation 'com.android.volley:volley:1.1.1'
    implementation 'com.muddzdev:styleabletoast:2.2.3'
}
```

Continúo describiendo la actividad loginActivity.



La pantalla de login sólo posee dos cajas de texto para login y contraseña y un botón para iniciar sesión, que se declaran al comienzo de la clase. Después se instancian y se le dice al botón lo que tiene que hacer, en este caso, llama al

método iniciar sesión, declarado un poco más abajo. Lo que hace este método es llamar al login.php y hace una consulta en la base de datos para buscar al login que se le pasa, con permisos entre 1 y 3 (4 no, porque el permiso 4 es para super administrador) y la contraseña. Si encuentra al usuario entonces la variable encuentrausuario que inicialmente estaba a false cambia a true y almacena todos los datos.

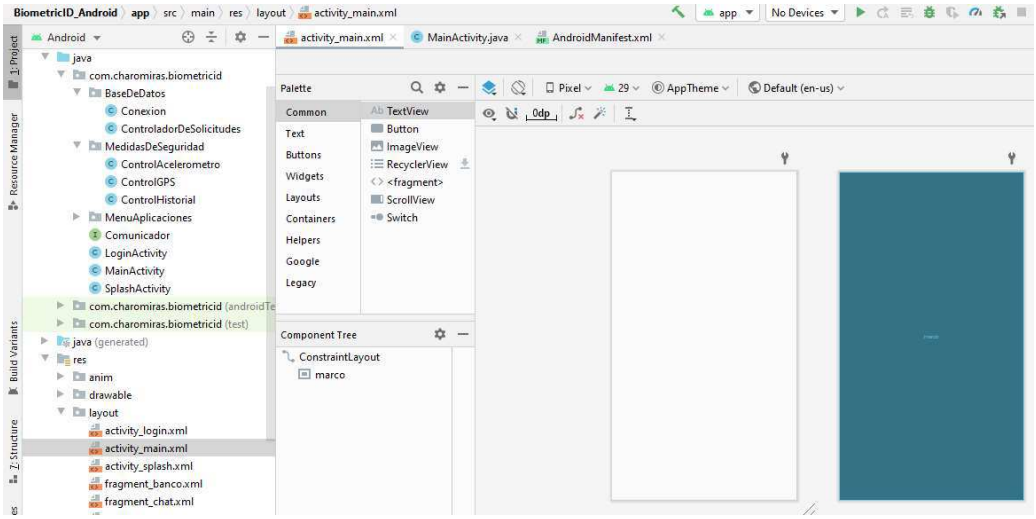
```
public class LoginActivity extends AppCompatActivity {

    Button entradaBoton;
    TextView entradaUsuario;
    TextView entradaContrasena;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_login);
        getSupportActionBar().hide();

        entradaBoton = (Button) findViewById(R.id.entradaBoton);
        entradaUsuario = (TextView) findViewById(R.id.entradaUsuario);
        entradaContrasena = (TextView) findViewById(R.id.entradaContrasena);


        entradaBoton.setOnClickListener((view) → {
                IniciarSesion(entradaUsuario.getText().toString(),entradaContrasena.getText().toString());
        });
    }
```

```
    public void IniciarSesion(final String login, final String password){
        StringRequest stringRequest = new StringRequest(Request.Method.POST, Conexion.URL_LOGIN, new Response.Listener
            @Override
            public void onResponse(String response) {
                try {

                    JSONObject jsonObject = new JSONObject(response);
                    JSONArray datosArray = jsonObject.getJSONArray( name: "usuario");
                    String inicioSesionCorrecto = jsonObject.getString( name: "login");

                    if (inicioSesionCorrecto.equals("false")){
                        StyleableToast.makeText( context: LoginActivity.this,  text: "La contraseña o el usuario son incor
                    }else if (inicioSesionCorrecto.equals("true")){

                        JSONObject o = datosArray.getJSONObject( index: 0);
                        SharedPreferences.Editor prefSave = getSharedPreferences( name: "MisPreferencias", getApplicat
                        prefSave.putString("nombre", o.getString( name: "nombre"));
                        prefSave.putInt("permisos", o.getInt( name: "permisos"));
                        prefSave.commit();

                        startActivity(new Intent( packageContext: LoginActivity.this, MainActivity.class));
                    }
                } catch (JSONException e) {
                    e.printStackTrace();
                }
            }
```

```
        }, new Response.ErrorListener() {
            @Override
            public void onErrorResponse(VolleyError error) {
                error.printStackTrace();
                StyleableToast.makeText( context: LoginActivity.this,  text: "Ha ocurrido un error.\nNo se ha podido conec
            }
        }){
            protected Map<String , String> getParams() throws AuthFailureError {
                Map<String , String> params = new HashMap<>();
                params.put("login", login);
                params.put("password", password);
                return params;
            }
        };
        ControladorDeSolicitudes.getInstance(getApplicationContext()).addToRequestQueue(stringRequest);
    }

    public void AbrirMainActivity(View view) {startActivity(new Intent( packageContext: LoginActivity.this, MainActivity
}
```

Al método se le pasan los parámetros login y password con el getparams() y los envía. Si inicioSesionCorrecto es false, se llama a la librería StyleableToast y aparece el mensaje “¡La contraseña o el usuario son incorrectos!”. Si, por el contrario, encuentra al usuario, guarda en mis preferencias con getSharedPreferences, el nombre del usuario y sus permisos para poderse utilizar las veces que se quieran. Acto seguido cambia de loginActivity a MainActivity. Si mientras estamos intentado conectar, perdemos la conexión a internet o hay algún problema, entonces se mostraría el mensaje “Ha ocurrido un error, no se ha podido conectar con el servidor”.

Si se echa un vistazo al fichero activity_main.xml vemos que está blanco. Esto pasa porque sobre esta pantalla se van a lanzar todos los botones: los controles del acelerómetro, los controles del GPS, los controles del historial de aplicaciones y los del libro. Es la pantalla base.

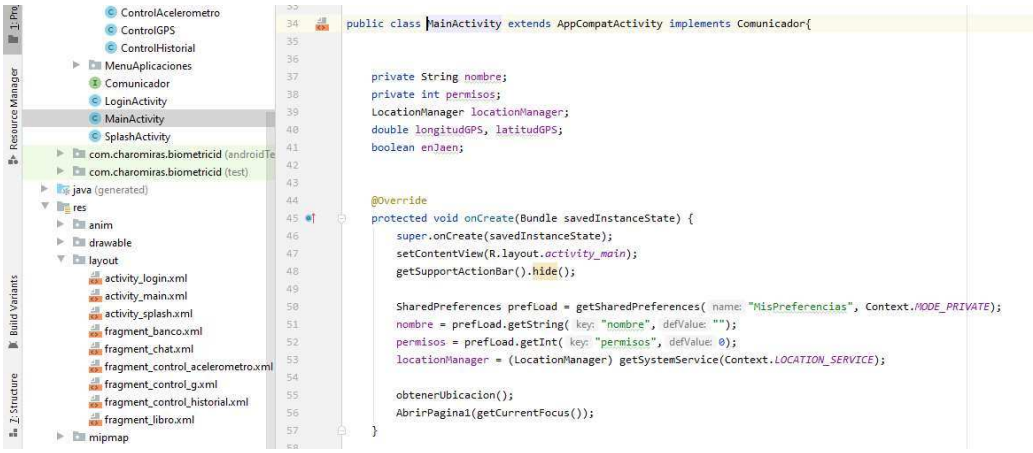


Analicemos a continuación que hace la actividad MainActivity.

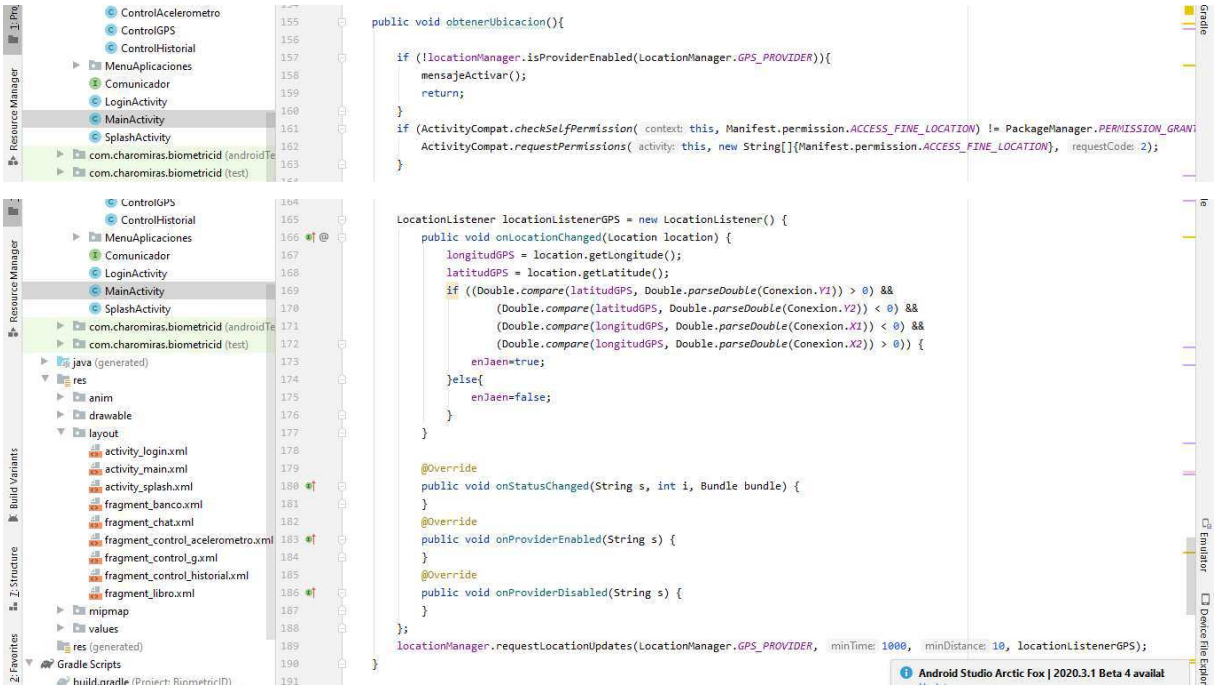
Al inicio se declaran las variables nombre, permisos, una variable para la localización, la longitud y latitud del GPS, y un booleano para comprobar si estamos o no en Jaén.

Lo primero que se carga es el método onCreate. Como inciso, explicamos que se usa getSupportActionBar().hide() para esconder una barra que viene por defecto en Android, y visualmente no nos interesa. Se cargan los datos de

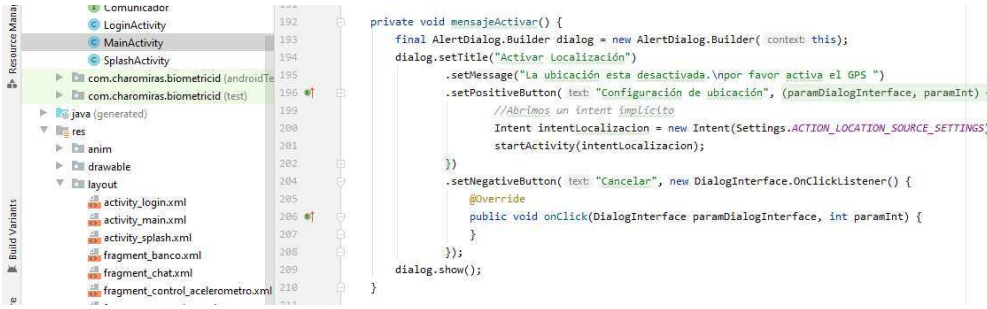
nombre y permisos guardados en preferencias (es la única forma de recoger los datos) y la localización.



Seguidamente se llama al método obtenerUbicacion() para llenar la variable enJaen, que se había declarado al inicio.



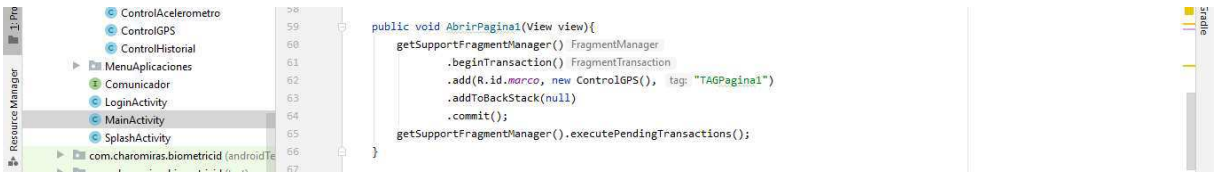
Lo primero que se solicitan son los permisos de ubicación que para continuar deben ser aceptados, si no, mostraría mensaje de error.



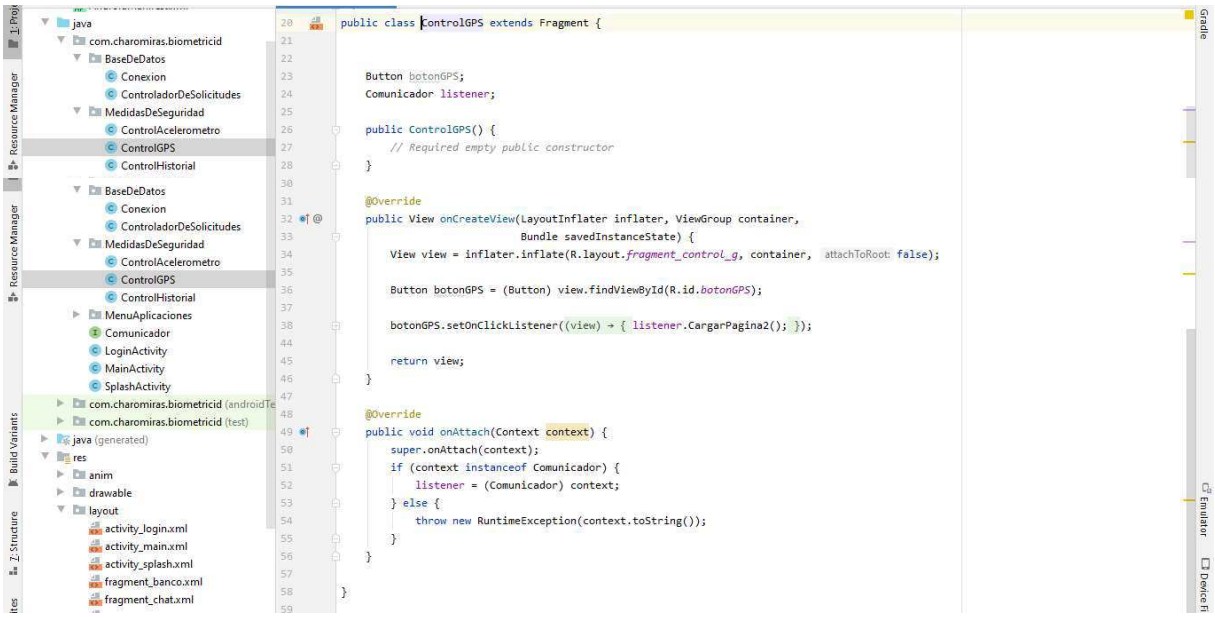
Este método compara la longitud y la latitud que contiene en ese momento el GPS con las coordenadas que previamente se han declarado para la zona de acceso. Estas coordenadas se han declarado en la clase Conexion(), que contiene cuatro puntos que delimitan la zona donde el acceso está permitido.

Si las coordenadas donde se localiza el terminal móvil son correctas, la variable enJaen pasaría a ser true. En caso contrario false. La localización del terminal móvil se actualiza cada segundo con una tolerancia de 10 metros.

Después de comprobar la variable enJaen, se llama al método AbrirPagina1() que lo único que hace es comprobar que el GPS es correcto.



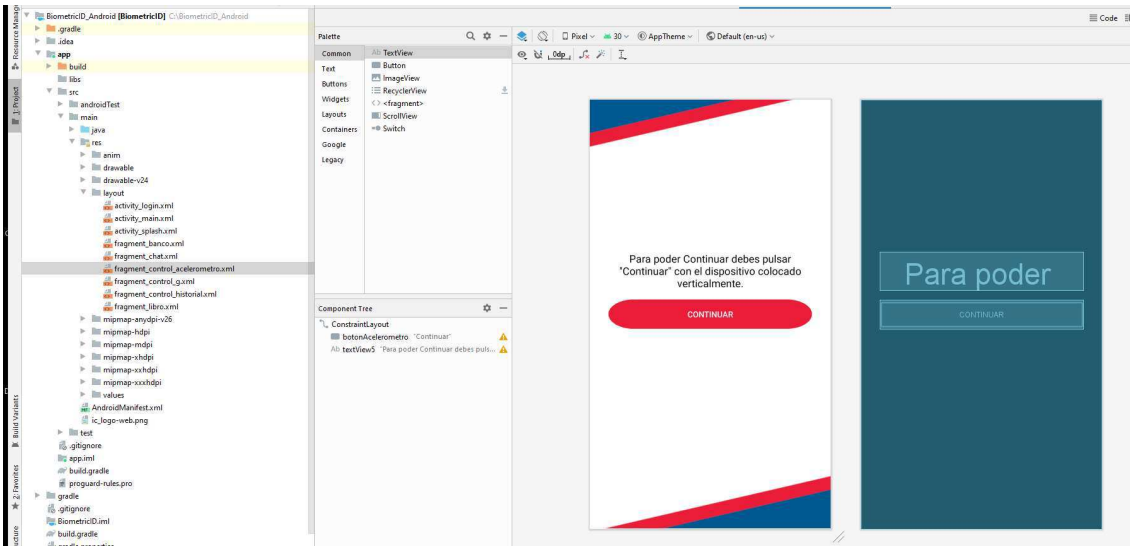
Para ello llama a ControlGPS() que lo único que tiene es un botón, ya que los controles se realizan en CargarPagina2().



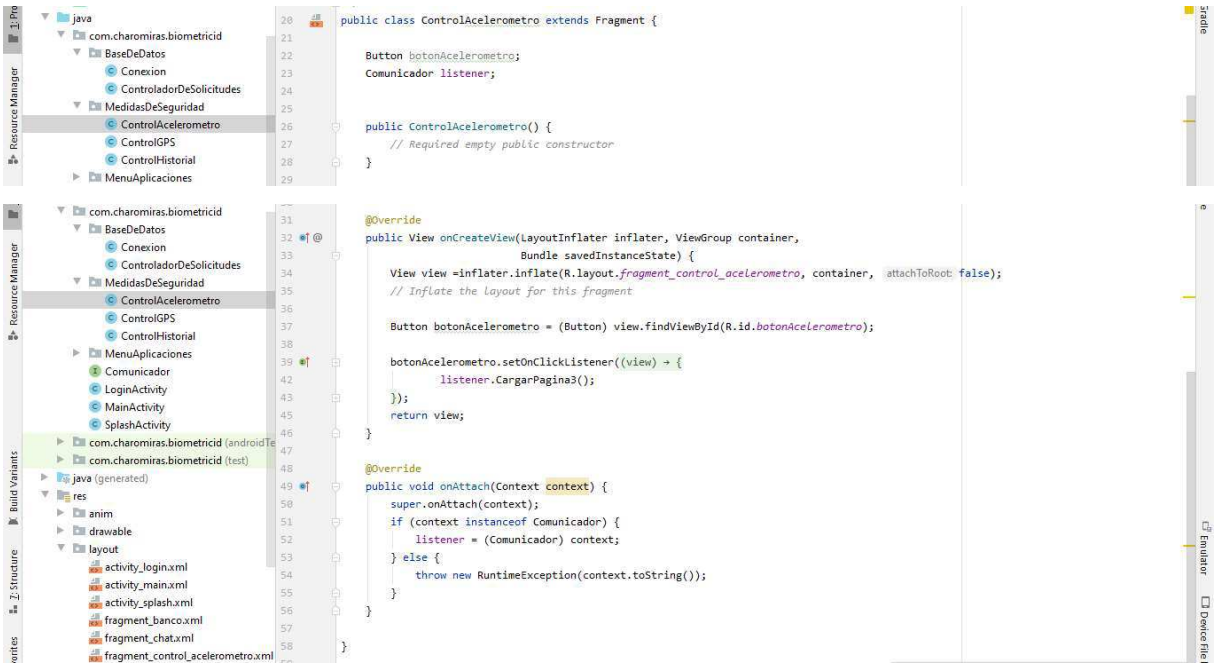
Observamos ahora la función CargarPagina2(). Si la variable 'enJaen' es true, es decir, es verdad entonces, si el usuario tiene permiso, carga la siguiente página que sería el acelerómetro. Para ello llama a la función ControlAcelerometro (). Si, por lo contrario, el usuario no tiene permisos, llamaría a la siguiente página, que es la función CargarPagina3().

Si la variable 'enJaen' es falsa, directamente es porque el usuario no se encuentra dentro de la zona delimitada para el acceso por GPS.

Suponiendo que el usuario está en la zona de acceso que se ha delimitado por el GPS, es decir, la variable ‘enJaen’ es true y que éste tiene permisos para acceder, entonces llama a ControlAcelerometro(), que lo único que tiene es un botón.

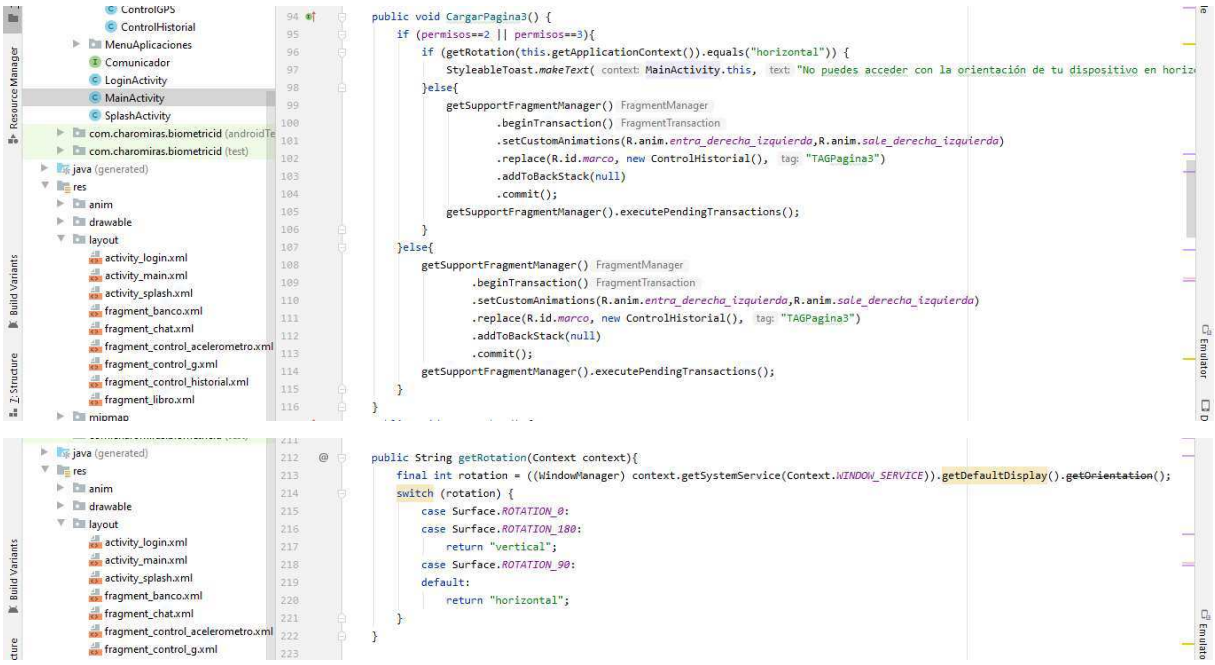


La funcion ControlAcelerometro() tiene un boton que lo único que hace es cargar el método CargarPagina3().



Si se observa el método CargarPagina3(), la primera comprobación que realiza es los permisos del usuario. Si el usuario tiene permisos para acceder (debe tener permisos de nivel 2 o 3, ya que con el permiso de nivel 1 no es válido)

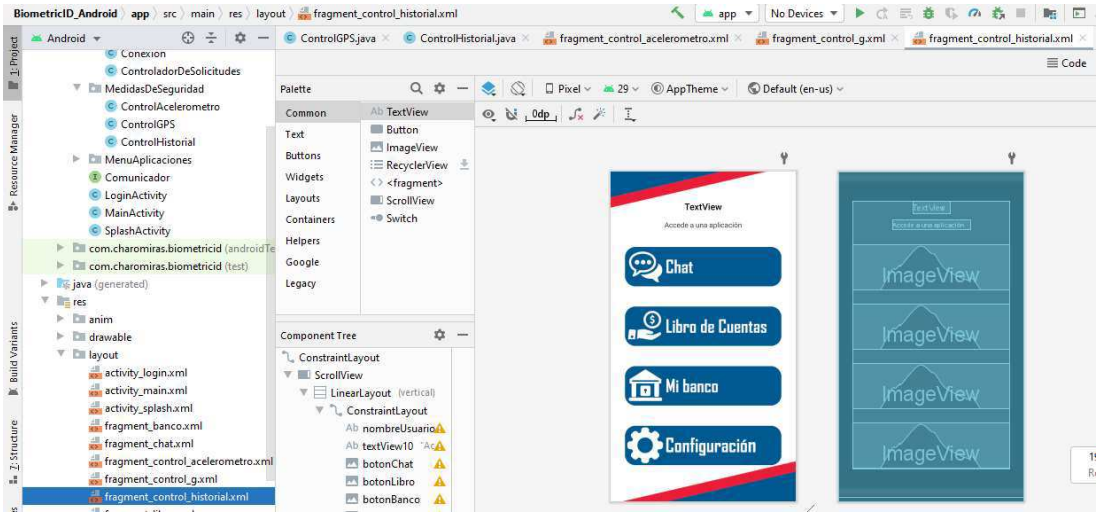
entonces se comprueba el sensor del acelerometro. Para ello usa getRotation() y comprueba que sea horizontal, si es vertical lanzaría un mensaje de error de horientación del terminal móvil o tableta.



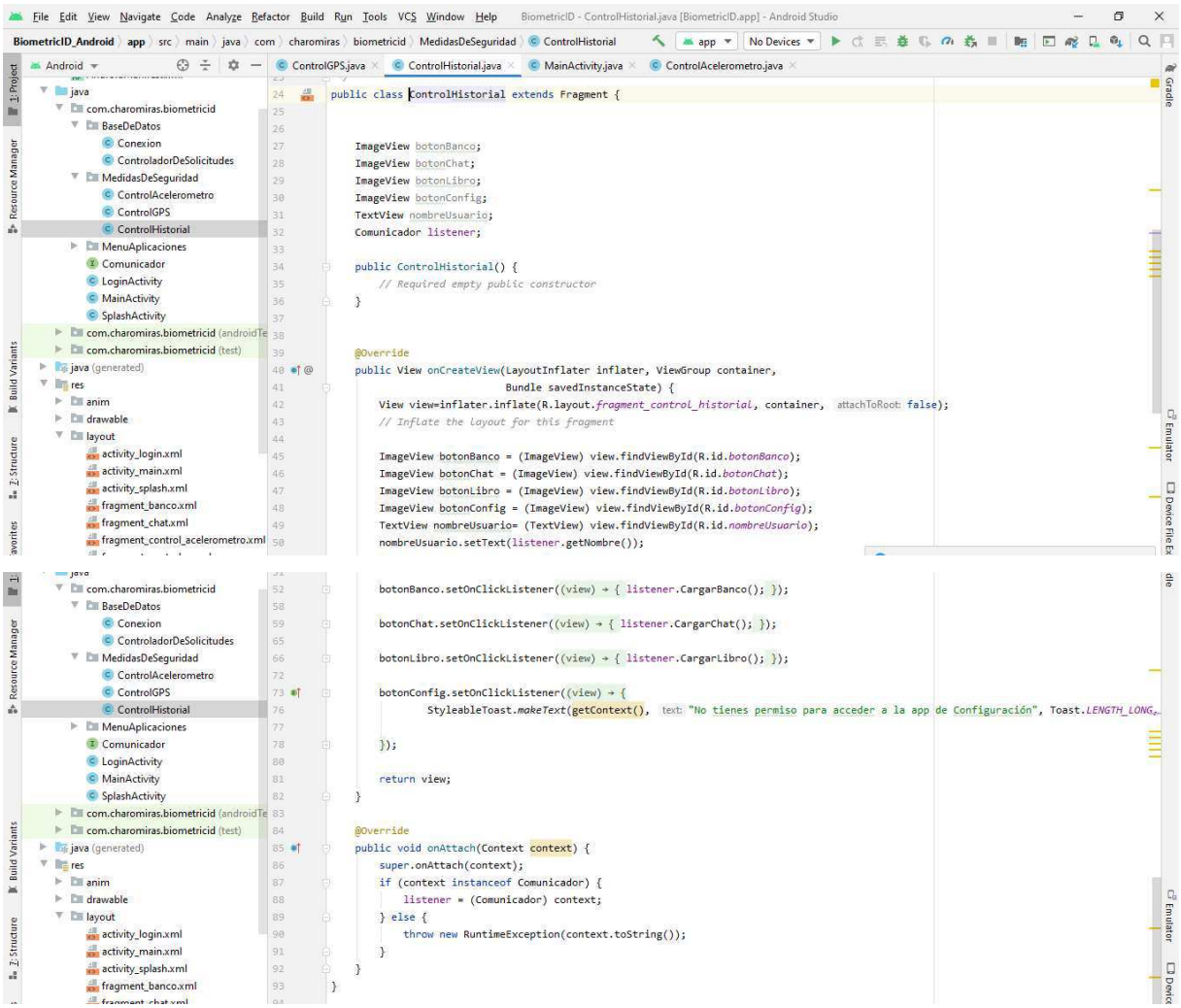
```
public void CargarPagina3() {
    if (permisos==2 || permisos==3){
        if (getRotation(this.getApplicationContext()).equals("horizontal")) {
            StyleableToast.makeText( context: MainActivity.this,  text: "No puedes acceder con la orientación de tu dispositivo en horiz
        }else{
            getSupportFragmentManager() FragmentManager
                    .beginTransaction() FragmentTransaction
                    .setCustomAnimations(R.anim.entra_derecha_izquierda,R.anim.sale_derecha_izquierda)
                    .replace(R.id.marco, new ControlHistorial(),  tag: "TAGPagina3")
                    .addToBackStack(null)
                    .commit();
            getSupportFragmentManager().executePendingTransactions();
        }
    }else{
        getSupportFragmentManager() FragmentManager
                .beginTransaction() FragmentTransaction
                .setCustomAnimations(R.anim.entra_derecha_izquierda,R.anim.sale_derecha_izquierda)
                .replace(R.id.marco, new ControlHistorial(),  tag: "TAGPagina3")
                .addToBackStack(null)
                .commit();
        getSupportFragmentManager().executePendingTransactions();
    }
}
```

```
public String getRotation(Context context){
    final int rotation = ((WindowManager) context.getSystemService(Context.WINDOW_SERVICE)).getDefaultDisplay().getOrientation();
    switch (rotation) {
        case Surface.ROTATION_0:
        case Surface.ROTATION_180:
            return "vertical";
        case Surface.ROTATION_90:
        default:
            return "horizontal";
    }
}
```

Si todo es correcto y la posicion es vertical, se abre la siguiente página que es el control del historial. Observamos que tiene la página ControlHistorial().



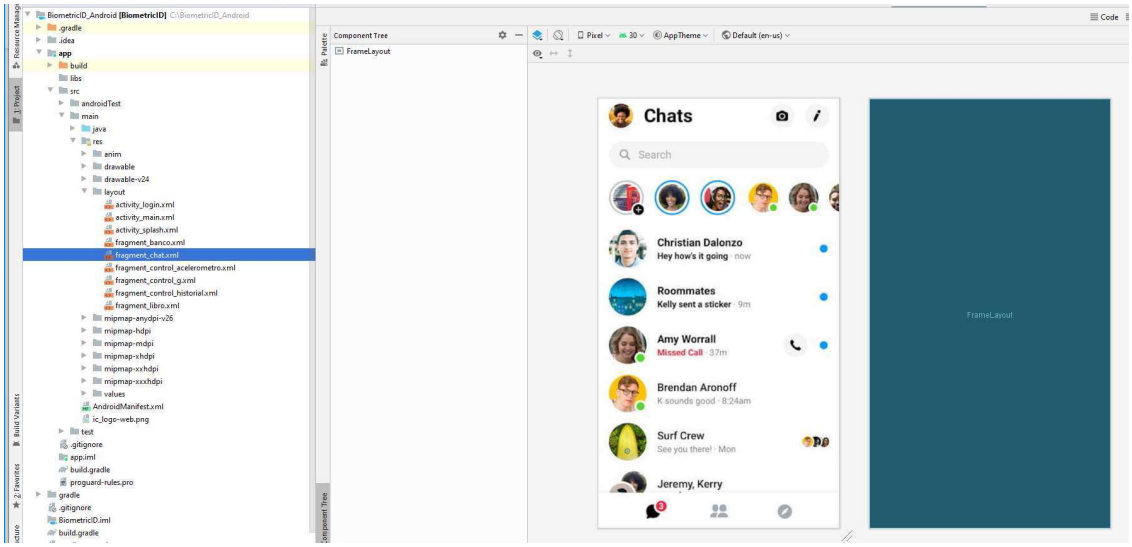
Lo primero que se hace es instanciar todos los botones y el nombre del usuario, para que se muestre en la pantalla. Cada botón va a llamar a un método: CargarBanco(), CargarChat() y CargarLibro().

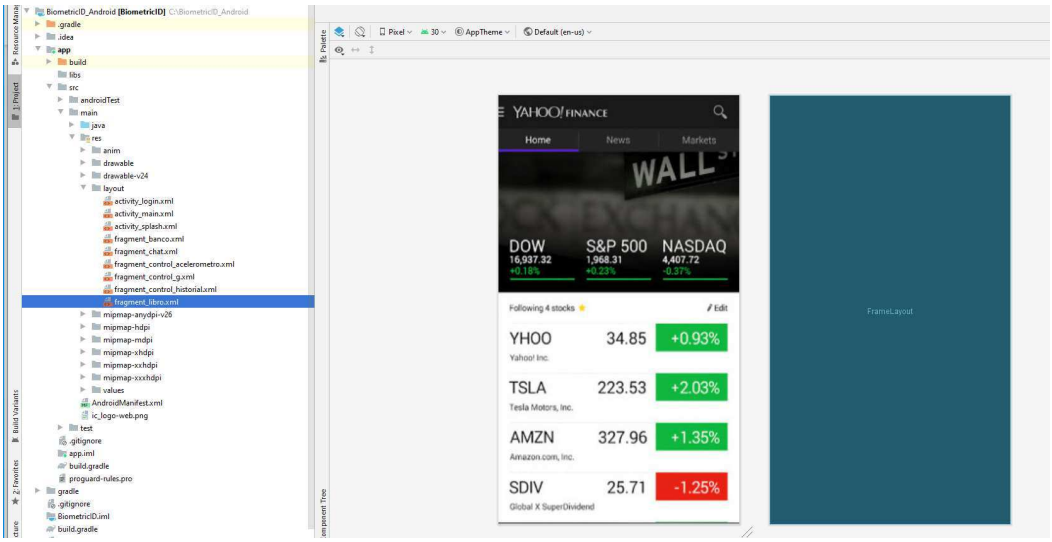


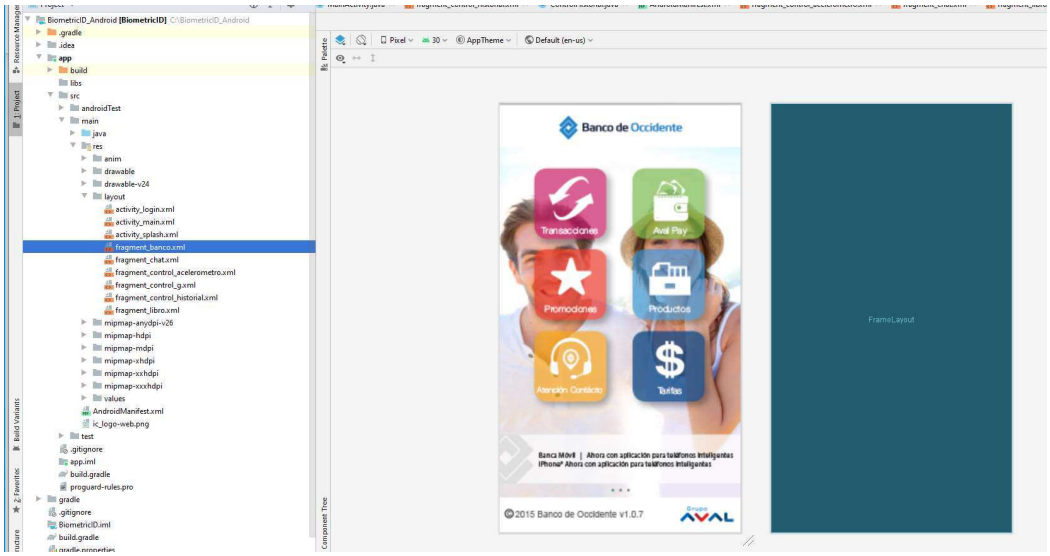
CargarChat() carga la página Chat(), no comprueba permisos porque todos los usuarios pueden acceder al chat, independientemente del nivel de permisos que

posea el usuario. CargarLibro(), primero comprueba que el usuario tenga permisos de nivel 2 o 3 para poder acceder, y si los tiene, entonces llama a Libro(). Y CargarBanco() comprueba que el usuario tenga permiso de nivel 3 y si lo tiene entonces llama a Banco().

Chat() mostraría en la pantalla del smartphone el chat, Libro() mostraría el libro de cuentas y banco() muestra el acceso al banco.







4.1.2. Modelo de Identificación

La aplicación desarrollada es una aplicación diseñada para sistemas operativos Android, que va enlazada junto a una aplicación web, basada en php, con acceso a una base de datos, donde se gestionan los usuarios y los permisos que tienen asociados cada uno de ellos.

Ilustración 4.1: Icono de la Aplicacion

A continuación se muestra el Inicio de sesión de la aplicación web.

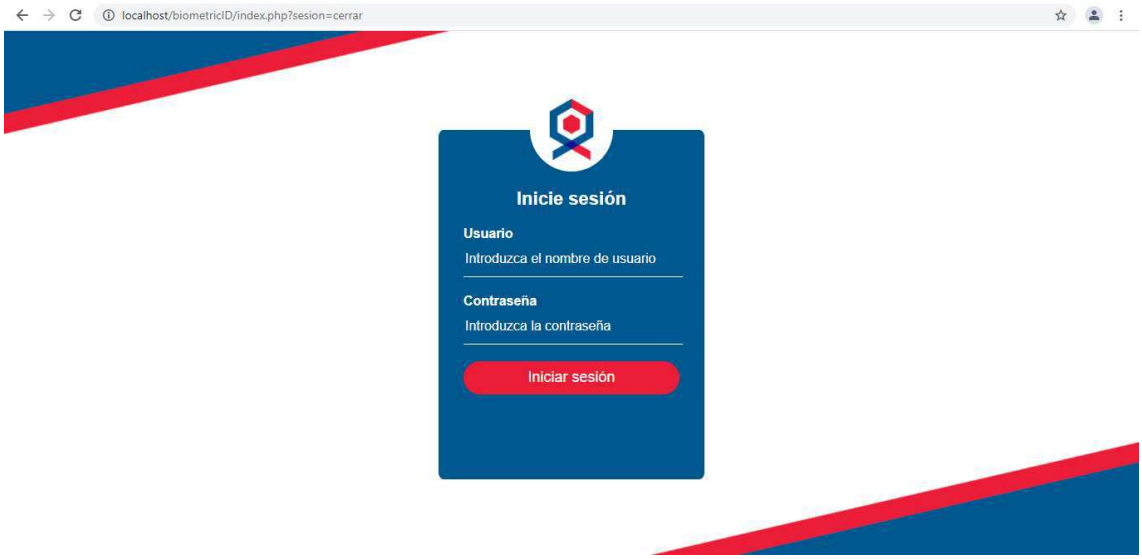


Ilustración 4.2: Inicio de sesion web

Para acceder al portal web, se usará el usuario administrador, que es el que tiene potestad para cambiar los permisos a todos los usuarios. En este caso el usuario es charo y la clave es 1234.

Ilustración 4.3: Panel del Control phpmyadmin - tabla usuarios

Ilustración 4.4: Ventana sistema de control web

En una lista desplegables se muestras las distintas opciones para elegir el usuario que deseamos modificar. Seguidamente aparece otra lista desplegable con los permisos que hay disponibles.

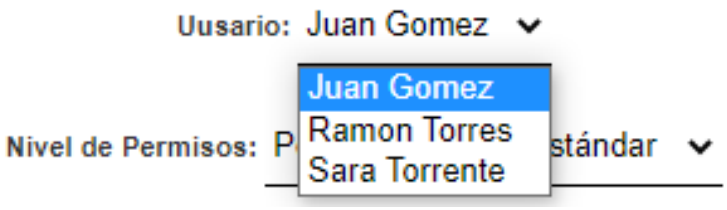


Ilustración 4.5: Listado de usuarios

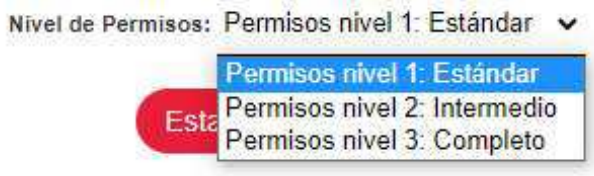


Ilustración 4.6: Listado de permisos

Una vez establecidos los permisos para cada usuario, ya se está en disposición de probar los accesos en la aplicación instalada en el terminal móvil.

Accedemos a la App y nos aparece la pantalla de bienvenida con una duración de segundos y automáticamente después, aparece la pantalla para loguearse. Intentamos loguearnos.

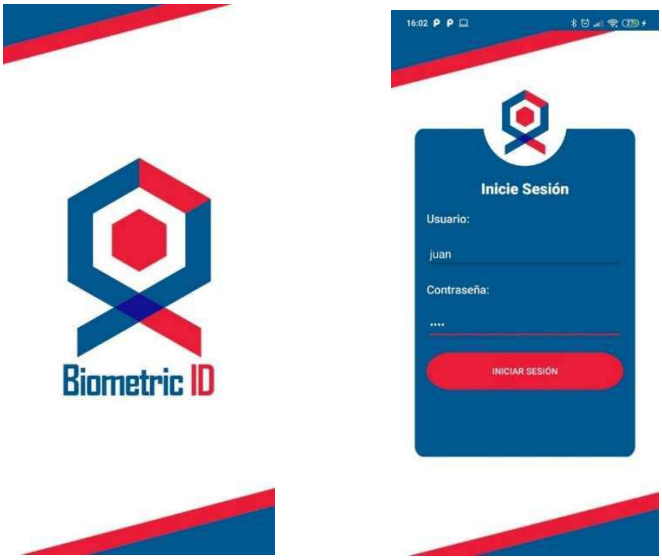


Ilustración 4.7: Pantalla de Bienvenida para smartphone y tablet

Ilustración 4.8: Inicio de Sesión

Si no se conecta con la base de datos nos mostraría el siguiente error:

Ilustración 4.9: Error al conectar en servidor

Si se introducen los datos del login erroneos también aparecería el siguiente mensaje:

Ilustración 4.10: Login erroneo

De lo contrario, si accedemos con el login correcto, nos pedirá permisos para acceder a la ubicación. Esto solo se pedirá la primera vez.

Ilustración 4.11: Solicitud de permisos de ubicación

Si el usuario tienes permisos de nivel 1, pedirá la localización del GPS que esté en la ubicación determinada para el acceso.

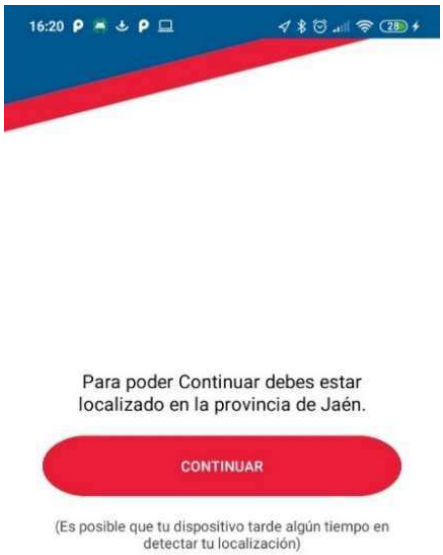


Ilustración 4.12: Localizacion del GPS

Si por el contrario, el usuario no se encuentra en la zona delimitada para el acceso de GPS, en nuestro caso Jaén, nos daría el siguiente error:

Ilustración 4.13: Error de localizacion

Vamos a suponer que hemos accedido a nuestra aplicación con el login deseado. En nuestro caso sería con el login de Juan, que tiene sólo permisos de nivel 1, es decir, sólo necesitaría estar en zona de GPS para el acceso y sólo tiene acceso a Chat. Por tanto, nos aparecería la siguiente pantalla con el menú de nuestro smartphone:

Ilustración 4.14: Acceso pantalla principal

Como el usuario que ha accedido tiene nivel 1, solo tendrá acceso a la app Chat, por lo que a las demás app nos daría error: mostramos las 3 pantallas dando error al acceso a la app de libro de cuenta, banco y configuración y acceso sólo a chat:

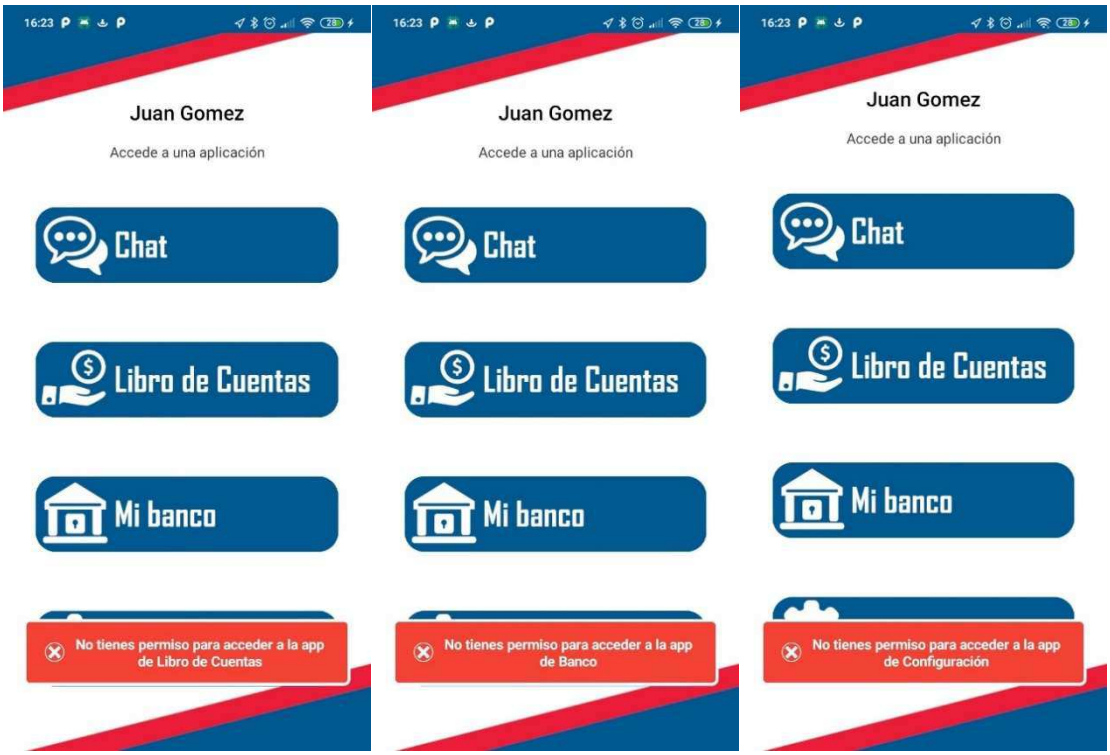


Ilustración 4.15: Mensajes de error de acceso a App

Ilustración 4.16: Acceso al chat

Procedemos ahora al acceso de login con un usuario de nivel 2, donde el usuario tendría acceso a la app del chat y al libro de cuentas, pero no podría acceder a nada más. Sus requisitos de acceso son 2 niveles de seguridad: estar en la zona delimitada por el GPS y que el smartphone estuviera en posición vertical. A continuación se muestran los pantallazos del smartphone con los mensajes de error:

Ilustraciones 4.17 y 4.18: Mensajes de error

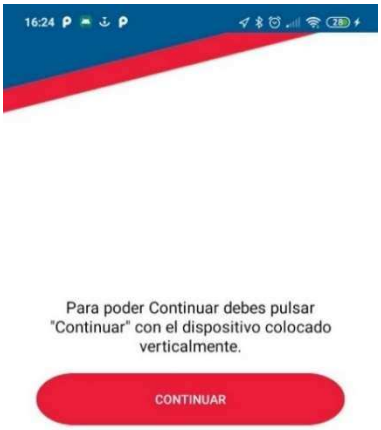
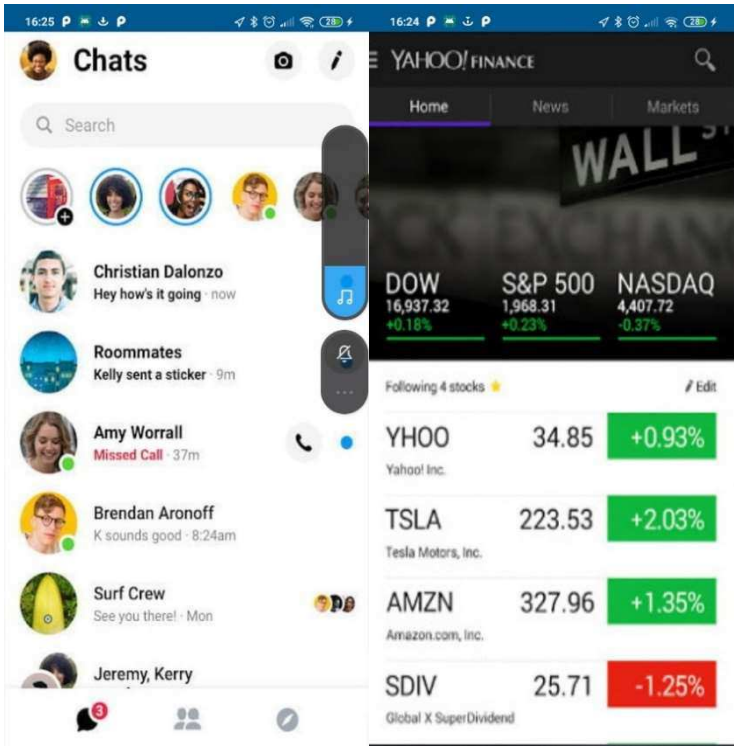


Ilustración 4.19: Mensaje aceptación para continuar

Ilustración 4.20: Mensaje error de acceso a banco

Ilustración 4.21: Mensaje sin acceso a configuración

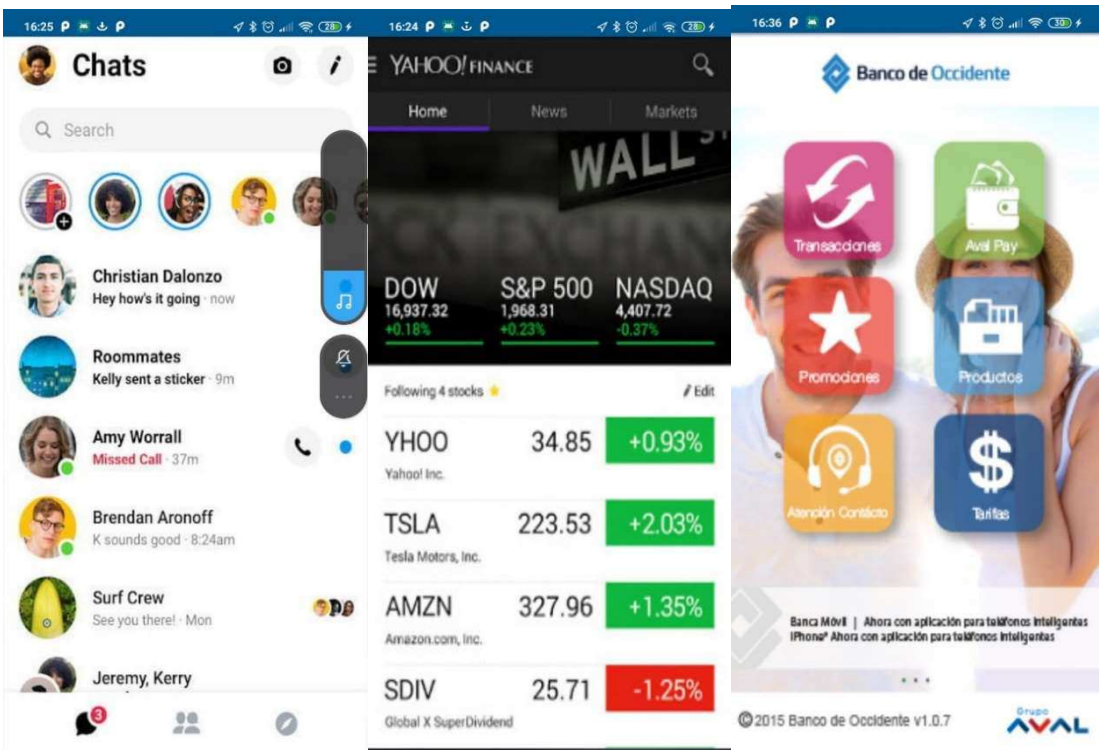


Ilustraciones 4.22 y 4.23: Acceso a App de chat y Banco

A continuación, procedemos a demostrar el acceso con un usuario de nivel 3, que tendría acceso a todo. En este caso damos permisos de nivel 3 al usuario Juan. Para ello, tendría que satisfacer los 3 niveles de seguridad dispuestos: estar en la zona de acceso delimitada por el GPS, el smartphone debería estar en posición vertical y, por último, debería ser una App usada habitualmente, y no una aplicación que no se use desde ese dispositivo móvil, como por ejemplo la aplicación del banco. Aun así, este usuario no podrá acceder nunca al menú de configuración, ya que no tiene permisos para ello.

Ilustración 4.24: Mensaje localización de GPS

Ilustración 4.25: Mensaje posición vertical del acelerómetro



Ilustraciones 4.26, 4.27, 4.28: Vistas de las diferentes Apps

Ilustración 4.29: Mensaje sin acceso a configuración

4.2. Validación del prototipo

Probamos el acceso con el usuario con permisos de nivel 1, en este caso es el usuario juan.

Conscientes de que nos situamos en Jaén, por lo que estaremos dentro de la zona delimitada para el acceso. Nos da varios mensajes de error de localización de GPS, ya que nuestro terminal de pruebas es bastante lento para actualizar la posición del GPS, por tanto, tendremos falsos negativos.

Tras varios intentos, en un tiempo de 3 minutos, se consigue el acceso.

Se ha realizado 5 intentos y se ha fallado 4 y acertado 1, por tanto, el porcentaje es 80% de falso negativo, FRR=0.8, frente al 20% de acierto. Esto es debido a la mala calidad del sensor GPS del terminal. Una mejora sería el cambio del terminal por otro con sensor de GPS de mayor precisión.

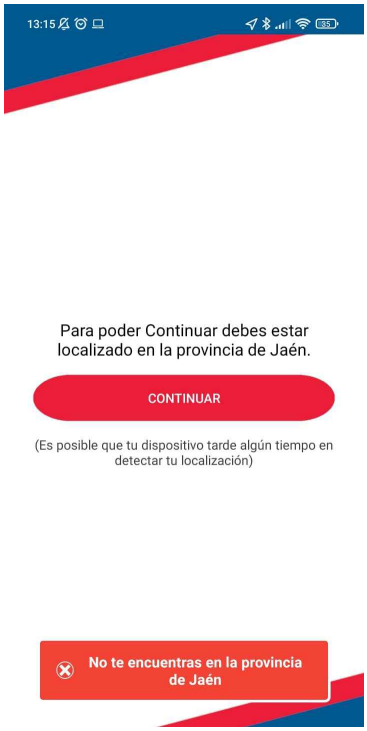
Una vez hemos accedido con el usuario Juan, probamos los accesos a las diferentes actividades.

- Acceso a chat con un 100% de acierto. Luego FRR es 0.
- No acceso a libro de cuentas, banco y configuración con 100% de acierto, es decir, nunca se accede, por lo que FAR = 0%.

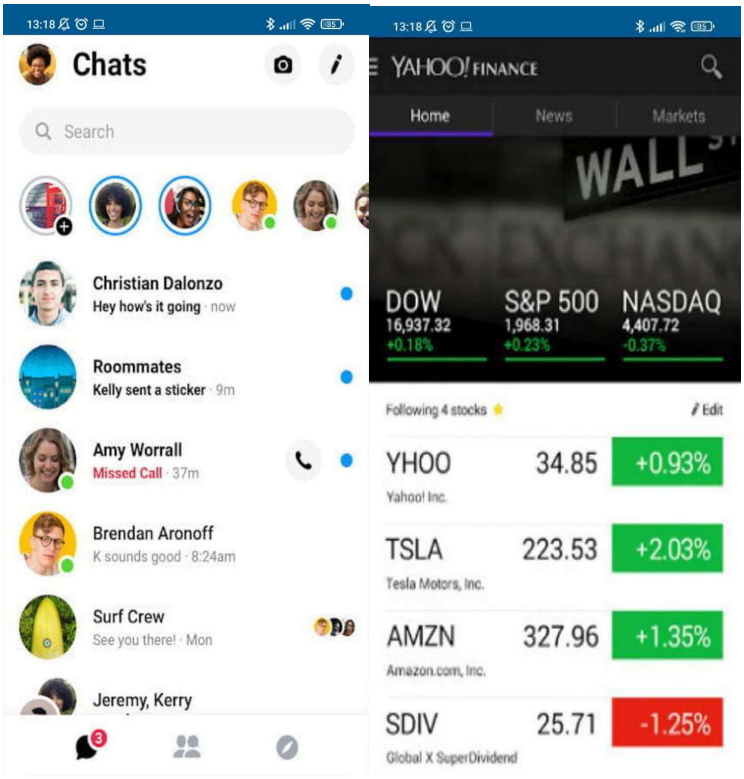
Se prueba ahora la aplicación con el usuario de nivel de permisos 2, es decir, con el usuario Ramón.

Suponiendo siempre que el usuario está en la zona de acceso por GPS, es decir, se encuentra en Jaén, intentamos acceder, pero volvemos a tener la misma tasa de fallo con el acceso por GPS como cuando se intentaba acceder

con el usuario juan. No vuelve a dar mensaje de error de localización de GPS aun estando dentro de la zona delimitada. Por tanto, tenemos la misma tasa de falso negativo, FRR=0.8, frente a una tasa de acierto del 20%. Tal y como se ha dicho anteriormente, debido a la mala calidad del sensor GPS del terminal de pruebas.

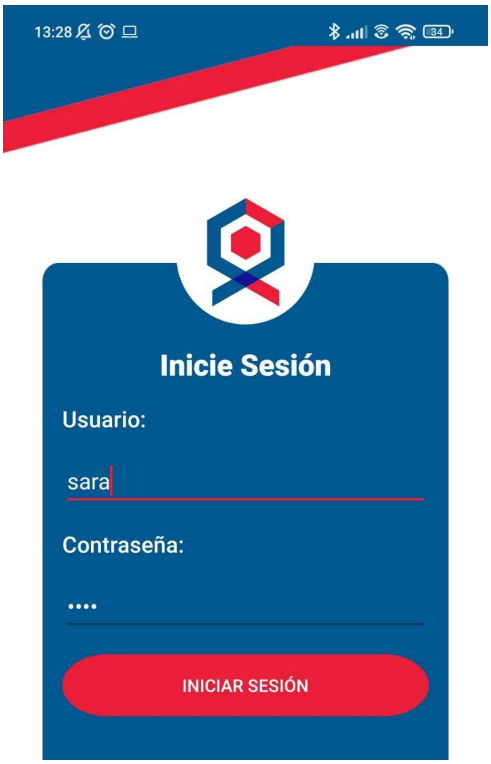


Una vez conseguido el acceso a la aplicación con el usuario Ramon, procedemos a probar el acceso a las diferentes actividades:



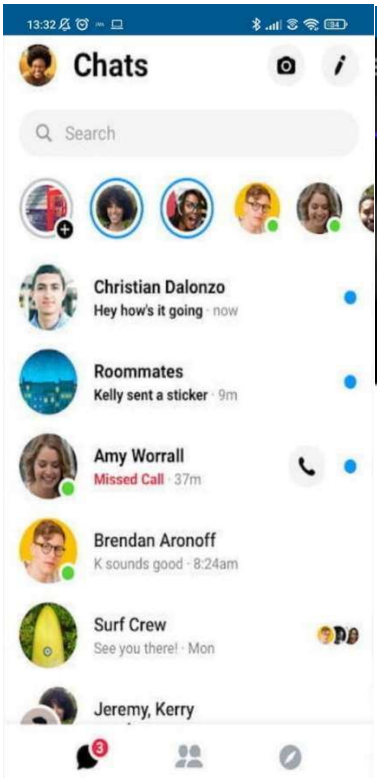
- Acceso a chat y libro de cuentas con un 100% de acierto, FRR = 0.
- No acceso a banco y configuración con 100% de acierto, es decir, nunca se accede, por lo que FAR = 0%.

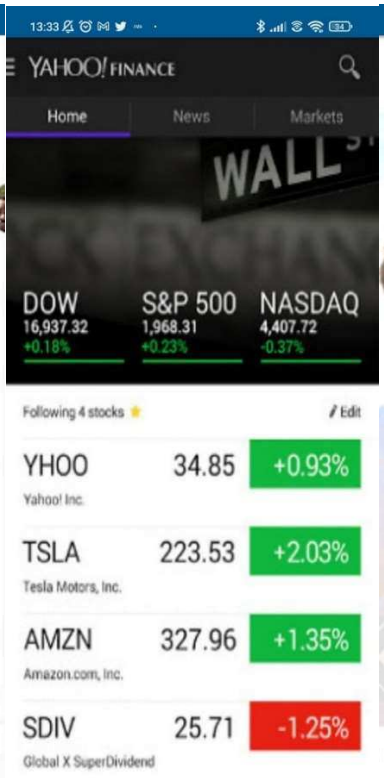
Probamos la aplicación con el usuario sara que corresponde con los permisos de nivel 3. Este usuario podrá acceder a todo excepto a configuración.



Volvemos a tener el mismo problema con el sensor del GPS que en los casos anteriores.

Una vez se ha accedido a la aplicación con el usuario sara, se procede a intentar acceder a las diferentes opciones de la aplicación. Se deberá poder acceder a todo excepto a configuración.





Efectivamente, tras realizar los intentos de accesos a las diferentes opciones de la aplicación, se consigue entrar a todo excepto a configuración, por tanto:

- Acceso a chat, libro de cuentas y banco con un 100% de acierto, FRR es 0.
- No acceso a configuración con 100% de acierto, es decir, nunca se accede, por lo que FAR es 0

Procedemos a finalizar las pruebas intentado acceder con cualquier usuario fuera de la zona delimitada por el GPS y después de varios intentos no se consigue acceder, por lo que tasa de aciertos es 100% y falso positivo, FAR = 0.

5. BORRADOR DEL PLAN DE MERCADO

Para realizar un plan de mercado o plan de marketing ajustado a nuestro producto, vamos a contemplar una serie de actuaciones.

Primeramente, realizaremos un análisis de la situación actual, es decir, la necesidad real que existe en los sistemas de identificación, para la inclusión de la biometría en estos sistemas identificativos. Como segundo punto, realizaremos un análisis de la situación que hay en el mercado sobre la existencia, de haberlas, de sistemas de identificaciones biométricas como la que proponemos nosotros, es decir, analizaremos los productos de la competencia.

5.1. Análisis de la Situación Actual

En la actualidad, casi todos los sistemas de identificación de usuarios requieren ya de varios sistemas de autenticación, ya sean 2FA o MFA.

Como ya hemos visto anteriormente, al principio empezaron a usarse basándose en algo conocido, como una contraseña y más tarde le siguieron los basados en algo que el usuario posee, por ejemplo, una tarjeta identificativa. En la actualidad, los sistemas de identificación más sofisticados usan conjuntamente varios factores de autenticación basados en una característica física o un comportamiento del usuario que se va a autenticar. La biometría ha revolucionado el mundo de los sistemas de identificación.

Por citar algunos ejemplos podemos comenzar nombrando el sistema de identificación que BBVA ha incorporado en su banca digital, en concreto, un sistema de identificación en su App basado en biometría. El usuario tiene la opción de elegir entre reconocimiento facial o huella dactilar. Dos características biométricas que garantizan la máxima tranquilidad al cliente.

Otro ejemplo es el sistema de llave digital que BMW ha presentado para el acceso a sus modelos iX, BMW Digital Key Plus[19]. Es una llave digital instalada en un smartphone de Apple, modelos compatibles con IPhone, con versiones de sistema operativo iOS 13.6 y WatchOS 6.2.8 o superior, que servirá para abrir y

[19] https://www.bmw.com/es/innovation/bmw-digital-key-el-iphone-como-llave-del-coche-segura.html

cerrar el coche, así como para encenderlo, todo ello con la máxima seguridad. Para ello se usará la App MyBMW, donde se añadirán los vehículos que posee el usuario. Una vez pareado el vehículo con la App, la llave digital quedará almacenada en la Apple Wallet. Iphone utiliza la tecnología Near Field[20], garantizando al máximo la protección de datos.

5.2. Análisis de la Competencia

A continuación, analizamos el mercado mediante una tabla, donde se expondrán los diferentes fabricantes/marcas que existen en la actualidad junto con sus prestaciones y/o funcionalidades que tienen dichos sistemas.

En una búsqueda sencilla en Internet, obtenemos diferentes soluciones de MFA (Multi-Factor Authentication) de las cuales expondremos sólo cuatro fabricantes.

Fabricante	Versión	2FA y/o MFA	Requiere intervención del usuario	Biometría	Uso en móvil	Licencia
Swivel Secure	Auth Control Sentry	2FA	Si	Si	Si	Coste por usuario
Microsoft Azure	Azure AD Multifactor	MFA	Si	No	Si	Coste por usuario o Coste por uso de autenticación
Cisco	Cisco Zero Trust – DUO	2FA	Si	No	SI	Coste por usuario
Inwebo	Inwebo	MFA	Si	No	Si	Coste por usuario

Tabla 5.1: Comparativa de soluciones que integran MFA

A grandes rasgos generales, casi todos los fabricantes estudiados anteriormente proponen las mismas soluciones en el mercado. Unas soluciones

[20] http://nearfieldcommunication.org/how-it-works.html

para la autenticación del usuario con 2FA o MFA compatibles con un centenar de aplicaciones, SSO, VPN, Proxy, IAM … con una integración rápida y sencilla. El segundo factor que podría utilizar el usuario en su autenticación se puede configurar según las necesidades de este, pudiéndose elegir entre token, código en SMS, llamada telefónica, OTP, biometría … de entre una gran variedad, donde el precio de la solución adquirida dependerá de la complejidad del factor elegido y del número de usuarios.

5.3. Modelo de Negocio

El modelo comercial elegido pasa por la estrategia de venta de esta solución desarrollada en este trabajo fin de máster, a los diferentes fabricantes de smartphone o tabletas con sistema operativo Android. Es decir, para diferentes marcas como Samsung, Huawei, Xiaomi, … Se vendería la solución a los fabricantes para que éstos incluyesen nuestra aplicación en todos sus terminales desde su fabricación. De esta manera, aumentaríamos el número de usuarios.

Realizando una comparativa de nuestra tecnología propuesta con las soluciones que hemos descrito en el punto anterior, podemos destacar varias diferencias que conllevan unas ventajas y desventajas entre ellas.

1. Todas las soluciones estudiadas pueden usarse en terminales smartphone y/o tabletas y en todas ellas se pueden utilizar 2 o más factores de identificación, lo que iguala a nuestra solución propuesta, no hay mejora.
2. En algunas soluciones anteriores si es posible escoger como factor de identificación la biometría al igual que es nuestra solución, aunque en otras no, por lo que en este punto podemos decir que nuestra tecnología obtiene una ventaja.
3. Pero la gran diferencia entre las soluciones que hemos comparado en el punto anterior y nuestra solución propuesta es el requerimiento de la intervención del usuario para su identificación. La transparencia para el usuario marca la diferencia y hace que nuestra tecnología sea más potente a la hora de la identificación.

Aumentamos la eficacia y la eficiencia, obteniendo otra ventaja frente a las otras soluciones comparadas.

Por tanto, podemos concluir, que nuestra solución tecnológica es más potente que las comparadas anteriormente.

Según el Observatorio Nacional de 5G[21], actualmente existen alrededor de 1281,2 millones de smartphone en el mercado mundial, y se espera llegando al 2025, que el crecimiento anual de smartphone será aproximadamente de un 4.3%. De esta cuota de mercado, casi el 50%, según Statcounter Global Stats, usan sistema operativo Android.

Ilustración 5.28: Cuota de mercado del SO en todo el mundo

Fuente: https://gs.statcounter.com/os-market-share/all/worldwide/2018

Para averiguar nuestros costes generales tendríamos que sumar el coste del desarrollo de la aplicación más es coste de la operación más el coste de la implantación, además del coste del mantenimiento evolutivo y mantenimiento correctivo. Una vez tengamos calculado el coste total, cabe averiguar los ingresos totales que se obtendrían para finalmente poder calcular los beneficios que se generan, en el caso de que los hubiera.

Para calcular los ingresos de media por usuario, tenemos que plantear primero como se van a generar dichos ingresos. Puesto que nuestra estrategia comercial es la venta directa de la licencia por usuario a los diferentes fabricantes de smartphone o tabletas con SO Android, se acapararía como máximo, casi el 50% de la cuota de mercado de terminales, siempre y cuando nuestro mercado fuera mundial, que no es el caso, por tanto, deberemos pensar que nuestra cuota

[21] https://on5g.es/

de mercado podría aspirar a un máximo de un 25% o 30%. Por lo tanto, nuestro ingreso sería por usuario que utilizase un terminal Android.

Una vez calculados los costes generales y los ingresos medios por usuario, debemos calcular el ARPU (Average Revenue per User) que es lo más importante, especialmente, en productos orientados al mercado residencial masivo. Como no es posible dividir el coste entre cada licencia y restárselo al PVP para calcular el AMPU, entonces, trabajamos con el coste total y un PxQ (ARPU multiplicado por el número de usuarios), de esta manera, calculamos la sencillamente los beneficios.

6. CONCLUSIONES Y TRABAJO FUTURO

Este TFM corresponde a un trabajo de investigación científica-técnica sobre cómo mejorar la identificación de usuarios que utilizan smartphone o tabletas, mediante el uso de la biometría. Éste es el propósito. No es un trabajo de ingeniería, eso sería una mejora tras este TFM.

He elegido esta investigación inclinada por el gran uso, y cada vez mayor, que los usuarios hacemos de los smartphones, ya que cada día aparecen nuevos modelos de terminales y aplicaciones que llenan dichos terminales.

En la actualidad, nuestra sociedad cada vez está más basada en el uso de aplicaciones y/o redes sociales. Aumentamos el uso que las personas hacemos de ellas y, por consiguiente, está conllevando a un modelo de sociedad en continuo cambio. Por ejemplo, antes necesitábamos ir a una farmacia o parafarmacia para comprar un bote de crema, y ahora podemos adquirirlo mediante una aplicación dedicada a ello. Antes alquilábamos un apartamento vacacional en una inmobiliaria y ahora podemos hacerlo mediante una aplicación. Antes teníamos que abrir un coche con una llave y ahora podemos hacerlo mediante un móvil. Estos casos son ejemplos de cómo ha ido evolucionando la sociedad mediante la tecnología, y en concreto, mediante las aplicaciones móviles. Pues bien, todo ello debería realizarse con una capa de seguridad, para que identifique a la persona correctamente y no a un usurpador. ¿Sería concebible que cualquiera puede abrir con su móvil nuestro coche? De ahí me surgió la idea, de la mejora de la identificación con la biometría.

6.1 Conclusiones

Una vez terminado el trabajo, debemos hacer una revisión para comprobar que se han cumplido todos los objetivos:

1. Concluimos, en base a lo estudiado anteriormente sobre nuestra solución y en comparativa con las soluciones que hemos podido encontrar de diversos fabricantes en el mercado, expongo, que la solución que se propone en este TFM, es totalmente diferente a lo encontrado en el mercado, ya que es una solución donde para la identificación de un

usuario en su terminal móvil, no es necesaria su intervención, es decir, la autenticación del usuario es transparente al humano y además usando varios factores de seguridad, por lo que aumenta al máximo la seguridad. Una solución donde se está usando MFA ajeno al conocimiento del usuario. Se puede decir que los objetivos descritos en los puntos 1.1.1 y 1.1.2 se han cumplido.

2. Tras la aparición de la biometría, el usuario no necesita poseer nada, ya que la autenticación biométrica es una característica física o de comportamiento de usuario, “como somos”. Por tanto, podemos concluir que se representa al usuario como único. Así pues, hemos cumplido el objetivo 1.1.3, ya que concluimos pues que podemos garantizar que la identificación en el terminal móvil solamente puede lograrse mientras esté en posesión del propietario o persona autorizada para su posesión y/o uso.
3. En el prototipo desarrollado, los factores de identificación usados son basados en sensores que contienen los terminales móviles de fábrica: el sensor de GPS, el acelerómetro y el historial de uso de App. Son factores de comportamiento del terminal móvil y por lo tanto son transparentes al usuario, no necesitan de su interacción, algo que beneficia la tarea de la identificación, siendo más eficaz y eficiente. Para poder acceder a las opciones de la App deberá, además de tener permisos para ello, estar dentro de la zona de acceso que se ha delimitado en unas coordenadas para el GPS, el terminal móvil deberá estar en la posición adecuada y acceso a la App habitual. Si todo ello se cumple, el usuario podrá tener acceso, de lo contrario, aparecerán una serie de mensajes de advertencia avisando al usuario. Todo ello, como se ha dicho anteriormente, transparente al usuario. Como consecuencia, vemos que nuestro objetivo número 1.1.4, de unir tres tecnologías (factores) diferentes en una misma solución, queda totalmente probado que los tres sistemas de identificación propuestos en nuestra solución son tecnológicamente compatibles y puede trabajar conjuntamente en un mismo producto.
4. En el prototipo se ha probado la identificación de 3 personas diferentes para el uso de una aplicación que contiene varias opciones: un chat, un libro de cuentas y el acceso a la banca digital. Según el nivel de permisos

que tenga cada usuario, éste podrá acceder a unas determinadas opciones de la aplicación, siempre y cuando cumpla con los requerimientos para su identificación, por tanto, cumplimos el objetivo número 1.1.5.

6.2 Trabajo futuro

Como mejora se podría continuar con un trabajo de ingeniería, como hemos dicho al principio.

Aumentos de las características u opción de la App desarrollada también sería otra mejora futura.

También podría mejorarse el sistema de identificación de GPS, con terminales smartphone que usasen sensores GPS más precisos y rápidos, lo cual reducirán la tasa de error, la tolerancia.

Otra mejora sería el aumento de usuarios que utilizasen la aplicación, añadiendo características a la aplicación, como, por ejemplo, identificación para el control horario, estaríamos aumentando el número de usuarios.

Otra nueva mejora sería la configuración del sensor de acelerómetro independientemente de cada usuario, es decir, para usuario que sea diestro o zurdo o para los que usan el smartphone modo horizontal o vertical, almacenar el estilo de uso del terminal para cada usuario, y no generalizarlo. Éstas y otras mejoras podrían realizarse en un nuevo trabajo de ingeniería para un nuevo diseño del prototipo.

La mejora de las posibilidades de conexión del GPS sería una buena opción. Es decir, ampliación de varias zonas de localización válidas para el acceso, como, por ejemplo, Málaga además de Jaén, como zonas válidas.

6.3 Comentario personal

Para terminar, quiero expresar una breve concusión personal sobre la realización de este TFM.

Dada la gran demanda de actividad que la sociedad está realizando en la descarga y/o el uso de las aplicaciones para terminales móviles y tabletas, es de obligado cumplimiento, hacer uso de ellas actuando siempre desde la seguridad y cautela en cada una de ellas, ya que, de manera directa, también han aumentado las usurpaciones y fraudes por el uso de estas aplicaciones. El trabajo de estudio que he realizado sobre la investigación para este TFM ha tenido como consecuencia, un gran trabajo de aprendizaje sobre la biometría. He aprendido cómo surgió la biometría, sus características y todos sus diferentes modos de aplicación y uso, que no son pocos. Todo ello ha conllevado, que, al término de este TFM, en la actualidad, he aumentado mi capacidad y percepción sobre la identificación de un usuario aplicando una capa de seguridad biométrica, de esta manera nos cercioramos de que el usuario es quién dice ser. Y lo mejor de todo ha sido, aplicar una capa de seguridad biométrica transparente al usuario, por lo que aumenta la eficacia y eficiencia.

Este aprendizaje me lleva a pensar cómo seguir aplicando la seguridad biométrica en la identificación de usuarios, no sólo en aplicaciones para terminales móviles y tabletas, sino para otros diferentes usos que hacemos las personas de forma cotidiana. Por ejemplo, el uso de la biometría en los hoteles[22]: identificación de nuestra huella dactilar en el registro del hotel (check-in), para su posterior uso. Así para acceder a las habitaciones y/o zonas comunes, bastaría con nuestra huella (alguna característica biométrica) y no haría falta ningún tipo de tarjeta o pulsera para identificarnos. A nuestra huella se le asignarían todos los permisos necesarios de accesos. Este proceso de identificación ya se está utilizando en el sector hotelero desde hace unos años, pero, aunque conlleva muchas ventajas tanto para el huésped como para el hotel, el costo para aplicar dicha tecnología aún es muy elevado.

En mi opinión, la identificación de usuarios con biometría está evolucionando a pasos agigantados, aumentando sus usos, por lo que no sería de extrañar que en pocos años dejen de usarse, por ejemplo, las llaves (de los vehículos, edificios, viviendas…) y/o las tarjetas (bancarias, de hoteles, de identificación laboral…).

[22] https://on5g.es/

Bibliografía

[1] Incibe CERT. (2015) Autenticación basada en contraseñas. https://www.incibe-cert.es/blog/autenticacion-basada-contrasenas

[2] Josep Albors (2020). WeliveSecurity. Qué es un ataque de fuerza bruta y cómo funciona. https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/

[3] Google. (2009) ReCaptcha. https://www.google.com/recaptcha/about/

[4] Google. (2018) ReCaptcha v3. https://developers.google.com/recaptcha/docs/v3

[5] Oficina de Seguridad del Internauta. (2019) El factor de autenticación doble o múltiple. https://www.osi.es/es/actualidad/blog/2019/02/27/el-factor-de-autenticacion-doble-y-multiple

[6] Instituto Nacional de Seguridad (2017). Dos mejor que uno: doble factor para acceder a servicios críticos. https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[7] Alphonse Bertillon (1853 – 1914). https://es.wikipedia.org/wiki/Alphonse_Bertillon

[8] Juan Vucetich (1858 – 1925). https://es.wikipedia.org/wiki/Juan_Vucetich

[9] Juan Vucetich. Dactiloscopía comparada (1904). https://upload.wikimedia.org/wikipedia/commons/2/21/Dactiloscop%C3%ADa_comparada.pdf

[10] John Daugman, "Iris Recognition for Personal Identification," The Computer Laboratory, University of Cambridge http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html.

[11] BeeDIGITAL. Historia y evolución del reconocimiento facial. https://www.beedigital.es/tendencias-digitales/historia-y-evolucion-del-reconocimiento-facial/

[12] Turk y Pentland. Eigenfaces for Recognition. https://www.face-rec.org/algorithms/pca/jcn.pdf

[13] Mejora del Algoritmo de Daugman para la localización del Iris (2012) https://www.researchgate.net/publication/269356134_Daugman's_Algorithm_Enhancement_for_Iris_Localization