TELELOGIN: UNA TÉCNICA DE AUTENTICACIÓN DE DOS VÍAS Y TRES FACTORES

TELELOGIN: A THREE-FACTOR TWO-PATH AUTHENTICATION TECHNIQUE

Rosendo Ayala Vaca
Universidad Quetzalcóatl en Irapuato, México
rayala@uqi.edu.mx

Claudia Zambrano Elizarraraz
Universidad Quetzalcóatl en Irapuato, México
czambrano@uqi.edu.mx

Adalberto Iriarte Solís
Universidad Autónoma de Nayarit, México
adalberto.iriarte@uan.edu.mx

Rafael Martínez Peláez
Universidad De La Salle Bajío, México
rmartinezp@delasalle.edu.mx

Recepción: 22/octubre/2019 **Aceptación:** 23/noviembre/2019

Resumen

En [Fujii, 2008] propusieron un sistema de autenticación utilizando un identificador de llamadas y dos métodos de autenticación, conocidos como Telelogin. En 2013, Fujii y Tsuruoka propusieron un método de autenticación de tres factores para solucionar los inconvenientes de seguridad en su trabajo anterior. Sin embargo, encontramos áreas de oportunidad para mejorar la seguridad utilizando autenticación basada en imágenes como contraseña biometría de huellas dactilares y posesión de un teléfono inteligente que combinados con algoritmos criptográficos incrementan la seguridad en todo el proceso. El resultado es una versión segura de los mecanismos de autenticación multifactor mediante telefonía.

Palabras Claves: Autenticación multifactor, contraseña única, huella dactilar, utilizar un dispositivo personal.

Abstract

In 2008, Fujii proposed an authentication system using a caller ID and two-authentication methods, known as Telelogin. In 2013, Fujii and Tsuruoka proposed a three-factor authentication method to remedy security drawbacks in their previous work. However, we found opportunities areas to enhance the security using image-based authentication as password, fingerprint biometric-based, and possession of a smartphone combining with cryptographic algorithms improve the security of the entire process. The result is a secure version of multifactor authentication mechanisms using telephony.

Keywords**:** *Bring your own device, fingerprint*, *multi-factor authentication, one-time password.*

1. Introducción

Una de las maneras más comunes para controlar el acceso a los sistemas informáticos es identificar quién está usando el dispositivo para entrar al sistema (probar la identidad y después, decidir qué privilegios gozan una vez identificados). De acuerdo con [Rhodes, 2013] la autenticación se define como:

> "*La autenticación es el proceso por el cual las personas prueban que son quien dicen ser. Está compuesta por dos partes, una parte pública de identidad (generalmente es el nombre de usuario), combinado con una respuesta privada (como una contraseña)*".

Para que alguien pueda autenticarse, se pueden utilizar los siguientes paradigmas de manera única o combinada:

- Algo que se sabe o *Something You Know* (SYK), se basa en algo que se conoce. Todas las personas usan contraseñas para acceder a los sistemas, pero desafortunadamente, algo que se conoce también puede ser algo que se olvida [Velásquez, 2018].
- Algo que se tiene o *Something You Have* (SYH), para evitar el riesgo de que el usuario pueda olvidar la contraseña se hace uso de un objeto, dispositivo

o artefacto que el usuario tiene, aún con esta manera de autenticación se tiene el problema de que el usuario pueda perder el [Velásquez, 2018].

- Algo que se es o *Something You Are* (SYA), una alternativa a la memoria o a mantener un objeto seguro es hacer uso de un rasgo físico de cada persona que los hace únicos, como la huella dactilar [Martinez, 2011].

Es importante mencionar que, ciertos sistemas requieren medidas de autenticación robustas y, por lo tanto, se utilizan mecanismos de autenticación multifactor. Un mecanismo de autenticación multifactor emplea dos o más métodos de autenticación buscando [Zahid, 2010]:

- Dificultar un ataque.
- Incrementar la certeza sobre la participación del usuario en el proceso de autenticación.

La contribución del presente artículo se divide en tres aportes. El primer aporte es la descripción de un sistema multifactor de dos vías. El segundo aporte es el análisis a dos propuestas de Telelogin desde su perspectiva de seguridad, evidenciando sus fallas de seguridad. El tercer aporte es la propuesta de un nuevo mecanismo de Telelogin, mejorando las vulnerabilidades de las propuestas previas.
Por lo tanto, el objetivo del presente trabajo de investigación fue diseñar y evaluar un nuevo mecanismo de Telelogin para mejorar las características de seguridad de dichos métodos de autenticación.

2. Métodos

Para realizar la presente investigación, se siguió la siguiente metodología. En primer lugar, se estudiaron las dos propuestas de Haruko Fujii publicadas en 2008 y 2013 para comprender su funcionamiento. En segundo lugar, se realizó un modelado de cada propuesta utilizando el lenguaje unificado de modelado o *Unified Modeling Language* (UML) para conocer la interacción entre las entidades. En tercer lugar, se realizó un análisis de seguridad a las propuestas de Haruko Fujii publicadas. El análisis realizado consideró las posibles vulnerabilidades en

diferentes etapas de cada propuesta, examinando sus carencias y fallas de seguridad. A partir de este punto, se diseñó y evaluó una nueva propuesta que mejora las vulnerabilidades y fallas de seguridad de las propuestas de Haruko Fujii.

Telelogin

Haruko Fujii propuso en 2008, un método de autenticación basado en los factores *SYK* y *SYH*. El factor *SYK* es una contraseña y una llamada utilizando un teléfono con identificador de llamadas como factor *SYH*. Lo innovador de este método fue el uso de medios físicos diferentes, puesto que el primer factor hace uso de la red IP y el segundo hace uso de la red PSTN (*Public Switched Telephone Network*) [Fujii, 2008]. A continuación, se presenta el análisis de seguridad.

El primer fallo de seguridad fue considerar el uso de una contraseña basada en texto debido a que existen diferentes ataques, tales como ataques por fuerza bruta, diccionarios, *keyloggers*, *man-in-the-middle* [Zahid, 2010] que, permiten descubrir la contraseña. De acuerdo con [Ayala, 2018] el problema más grave que tiene este mecanismo de seguridad es que algo que el usuario sabe es también algo que puede olvidar, por lo que se requiere un método de recuperación como puede ser utilizar la respuesta secreta a la pregunta de olvido de contraseña, la cual se ha utilizado por años, dando otro punto vulnerable a un ataque.

Al realizar una comparativa entre los estudios sobre hábitos en contraseñas presentados en [CSID, 2012], [Guccione, 2017], se revela que las conductas de los usuarios de un servicio no han cambiado significativamente en los últimos años al preferir el uso de contraseñas cortas, simples y nemónicas. De acuerdo con [Pastorino, 2017] expone las diferencias en los cambios de contraseña por parte de usuarios del año 2016 y el 2017 donde se evidencia que realizaron un esfuerzo mínimo por incrementar la seguridad de sus contraseñas, sin embargo, los contraseñas son predecibles debido a que incluyen pequeños cambios para cumplir con las auditorías básicas de seguridad actuales, las cuales incluyen uso de mayúsculas, minúsculas, números, buscando que el sistema acepte como válidos los contraseñas. Por ejemplo, los usuarios cambiaron la contraseña “Contraseña” por “Contraseña1234” o “qwerty” por “Qwerty01!”.

El segundo fallo de seguridad se encuentra con la realización de la realización de la llamada. De acuerdo con [Fujii, 2008], el usuario realiza la llamada y el servidor valida el número mediante el uso de un identificador de llamadas. En caso de encontrar el número en la base de datos, se considerará completada la autenticación del usuario.

El inconveniente encontrado, se basa en que puede ser altamente vulnerado mediante un ataque por *spoofing* telefónico [CONDUSEF, 2018]. En términos de seguridad informática, el *spoofing* se refiere a la suplantación de identidad por parte de quien comete un delito, es una treta utilizada para intentar obtener información personal y usarla de manera ilegal, uno de los tipos de fraude que ha ido en aumento es por teléfono [Kinnunen, 2012].

El objetivo del *spoofing* es ocultar la identidad real, existen varios tipos como los de DNS, IP, correo electrónico, sitio web y telefónico; para el caso del teléfono, una persona falsifica a propósito la información que será transmitida al identificador de llamadas del teléfono o dispositivo a llamar, de esta manera, al momento de recibir la llamada, la pantalla mostrará una identificación manipulada y no la real.

A partir de la propuesta, se desarrolló el diagrama de secuencia en UML, figura 1.

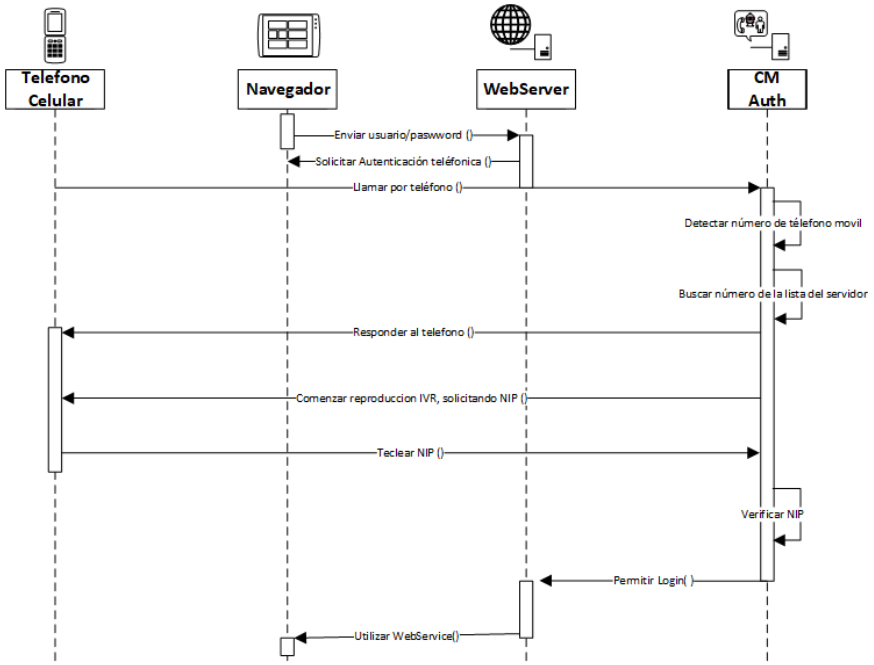


Figura 1 Diagrama de secuencia de autenticación Telelogin por doble factor.

Telelogin Mejorado

Con la finalidad de mejorar la seguridad de la propuesta presentada en 2008, Fujii y Tsuruoka agregaron un tercer método de autenticación utilizando como mecanismo de seguridad biométrico, la autenticación por voz [Fujii, 2013]. Sin embargo, se han encontrado las siguientes áreas de oportunidad.

En la nueva propuesta, se propone que una vez que el usuario realiza una llamada y el servidor de autenticación responde a la misma, solicita que el usuario diga una palabra o frase *n* de un banco de información finito anticipadamente registrado en el sistema. De haber una validación exitosa la verificación de la identidad será exitosa. Algunos de los inconvenientes que presenta un factor de autenticación por voz son los siguientes [Kinnunen, 2012], [Wu, 2012]:

La voz, como cualquier otro sonido se trata como una señal digital a la que es posible aplicarle un análisis de Fourier, del resultado analizar la voz como señal se consigue obtener el espectro característico de la persona, el cual, puede ser almacenado para más tarde comparar con otras señales en las que el registro, análisis y comparación, se va realizando en tiempo real, al punto de que cuando el usuario termina de mencionar su palabra o frase, el sistema ya fue capaz de analizar y contrastar contra la información en su base de datos para poder permitir o denegar el acceso. Por lo tanto, este método requiere una mayor potencia de cálculo que otros métodos biométricos, así como del uso de otras herramientas adicionales como algoritmos genéticos, lógica difusa, redes neuronales, inteligencia artificial que auxilien a los sistemas de reconocimiento de voz.

Los sistemas de reconocimiento de voz son susceptibles a condiciones similares en el ambiente como ruidos, ecos y reverberaciones que requieren del uso de filtros de frecuencias para identificar satisfactoriamente una serie de sonidos que reciben como señal de entrada. Durante este proceso, se analiza la entonación, la pronunciación de diptongos, la velocidad al hablar, así como las vocales.

Este tipo de sistemas trabajan con dos modelos, el primero de ellos es el modelo de texto dependiente que tiene un conjunto limitado de frases aptas para reconocer, como, por ejemplo: “mi nombre es Rosendo”, “la casa es de color azul”, “el auto es último modelo”, “el día es muy lindo” o “el patio es muy grande”. Por otra parte, se

encuentra el modelo de texto independiente que propone al usuario la pronunciación de ciertas palabras extraídas de un conjunto más amplio, por ejemplo, del siguiente texto [De Saint, 1956] que un usuario podría leer y grabar durante el registro de la voz:

> *"Conozco un planeta donde vive un señor muy colorado, que nunca ha olido una flor, ni ha mirado una estrella y que jamás ha querido a nadie. En toda su vida no ha hecho más que sumas. Y todo el día se lo pasa repitiendo como tú: "¡Yo soy un hombre serio, yo soy un hombre serio!"... Al parecer esto le llena de orgullo. Pero eso no es un hombre, ¡es un hongo!".*

El sistema de reconocimiento de voz, podría extraer y solicitar al usuario la pronunciación de una o más palabras que cumplan con las condiciones requeridas a contrastar. Como ejemplo se pueden mencionar: "planeta", "señor", "colorado, "flor", "estrella", "vida", "serio", "orgullo", "hombre", "hongo", entre otras.

En ambos métodos, al utilizar un banco finito de respuestas, la autenticación por voz puede ser objeto de un "*impersonation attack*", el cual consiste en reproducir palabras o frases previamente grabadas de un usuario legítimo para violar el reto presentado [Piotrowski, 2007].

Este mismo método, puede dar una alta tasa de falsos negativos, al no reconocer la voz de un usuario por la reducción del ancho de banda en la frecuencia de transmisión, por estados de ánimo o problemas de enfermedades otorrinolaringológicas y respiratorias. Se ha vuelto un problema continuo en que el usuario se encuentre obligado a repetir su frase de autenticación porque el sistema le deniega el acceso debido al error de reconocimiento de voz o *Wrong Error Rate* (WER) [Allan, 2017]. En la figura 2, se presenta el diagrama de secuencia de las mejoras realizadas por Fujii en la actualización de su esquema de Telelogin.

3. Resultados

A partir del análisis realizado a las dos propuestas de Fujii, se presenta una nueva propuesta con mejoras en el diseño.

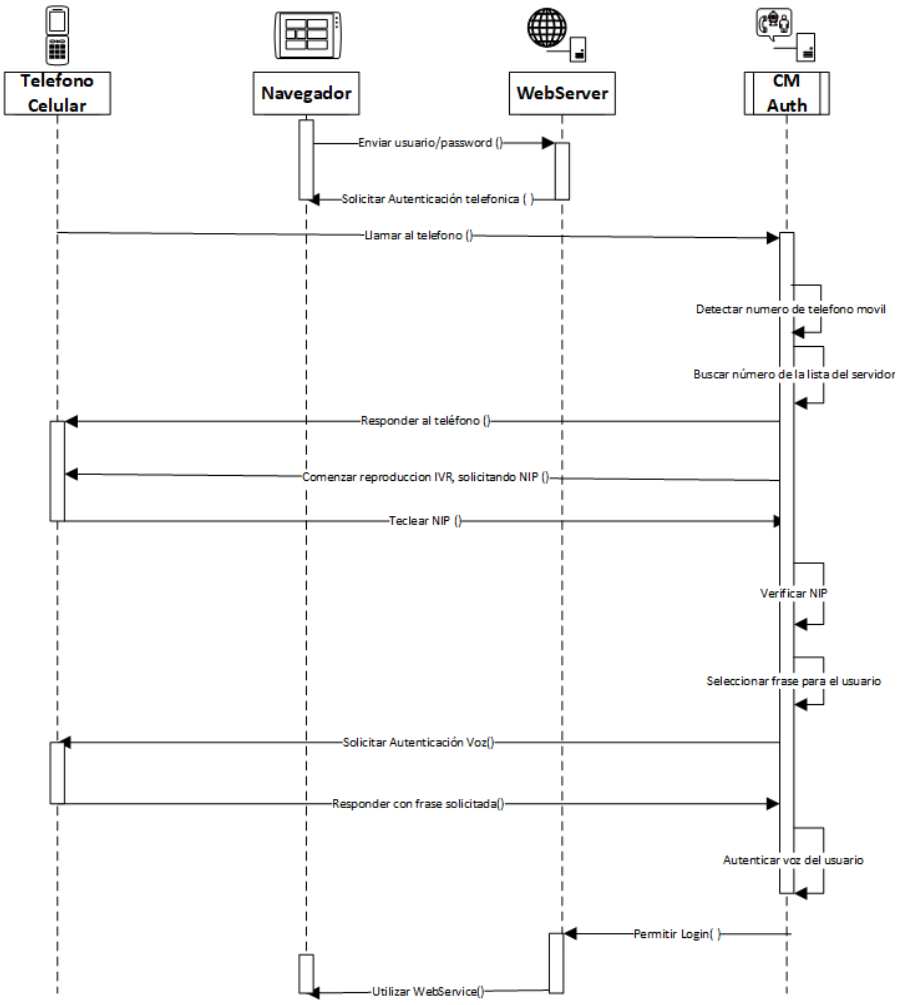


Figura 2 Diagrama de secuencia de autenticación Telelogin por triple factor.

Componentes Generales

La propuesta contempla el uso de los tres factores (*SYK*, *SYH*, *SYA*) con la finalidad de ofrecer un mecanismo seguro y robusto. Además, se considera utilizar las siguientes herramientas de seguridad [Schneier, 1996]: una contraseña de un único uso o *one-time password* (OTP), un sello de tiempo o *time stamping*, función *hash*, y una función *fuzzy hash*.

A continuación, se describe de manera general la propuesta. Todos los datos de identificación de los métodos *SYK* y *SYH* son sometidos a una función *hash* y se les incluye un sello *time stamping*; al método *SYA* se le aplica una función *hash* del tipo *fuzzy hash*.

Entidades

La propuesta contempla la participación de las siguientes entidades:

- Usuario: es la persona que desea utilizar el sistema de autenticación. El usuario es quien debe utilizar su dispositivo móvil para descargar la App, realizar el proceso de registro, llevar a cabo el proceso de autenticación, y mantener la confidencialidad de las contraseñas utilizadas.
- App: es la aplicación para dispositivos móviles que debe ser descargada por los usuarios para poder utilizar el sistema de autenticación.
- *Login Server*: es el servidor encargado de iniciar el proceso de verificación de identidad a partir de recibir la solicitud del usuario.
- *Data Base Server*: es el servidor encargado de mantener datos de autenticación de cada usuario. Entre sus funciones se encuentra proporcionar los desafíos al *Login Server*.
- *Call Manager Server*: es el servidor encargado en realizar la llamada al usuario en base al número de celular almacenado en el *Data Base Server*.

Supuestos

El mecanismo de autenticación propuesto tiene los supuestos:

- El usuario debe tener un dispositivo móvil con lector de huella dactilar.
- La conexión entre los servidores es a través de un canal de comunicación seguro.
- La App se encuentra disponible para los dos sistemas operativos más populares en teléfonos inteligentes.
- El Data Base Server se encuentra protegido ante intrusiones externas.

Fases de Registro

El mecanismo de autenticación propuesto requiere un proceso de registro para cada usuario.

El usuario debe descargar la App mediante el uso de sitios de distribución, como puede ser *Play Store*. Una vez descargada e instalada la App en el dispositivo móvil, el usuario debe seguir los siguientes pasos:

- Dar de alta el número del dispositivo móvil a través de la App para su almacenamiento en el *Data Base Server*.
- Seleccionar *tres* imágenes del banco de imágenes presentadas por la App, que serán utilizadas en el método *Image-Based Password*.
- Crear la plantilla de un dedo que será almacenado en el *Data Base Server*. La App deberá escanear tres veces el dedo seleccionado por el usuario para crear la plantilla [Dong, 2010].

Una vez concluido el proceso de registro, los datos son almacenados en el *Data Base Server* para su consulta por parte del *Login Server* durante las distintas fases de autenticación.

Fases de Autenticación

El proceso de autenticación propuesto consta de tres fases:

- La primera fase de autenticación se realiza con el método *Image-Based Password* como un reto para iniciar sesión en la aplicación móvil. Inicialmente, el usuario debe seleccionar *tres* imágenes del banco de imágenes en la etapa de registro.

  Las imágenes seleccionadas por el usuario serán almacenadas para verificar que el usuario es legítimo. Posteriormente, el usuario debe superar *tres* desafíos donde se mostrarán seis imágenes y el usuario debe marcar la imagen correcta, seleccionada en la etapa de registro [Sosa, 2018]. El usuario debe elegir correctamente cada imagen de los tres desafíos para que el sistema verifique la identidad del usuario por medio del enfoque *Image-Based Password*.
- La segunda fase de autenticación inicia después que el usuario supera la autenticación por *Image-Based Password*. En esta fase, la App envía el número de celular al *Login Serv*er. El *Login Server* recibe los datos y los envía al *Data Base Server* para comprobar los datos registrados en la base de datos. La conexión entre el *Login Server* y el *Data Base Server* se realiza a través de un canal de comunicación seguro. En caso que los datos de

identificación sean válidos, se responde con un mensaje de autenticación correcto que contiene el código OTP que deberá ser entregado al usuario.

En consecuencia, el *Login Server* envía el código OTP y la solicitud de una llamada al *Call Manager Server*. El Call Manager Server realiza una llamada a través de la red telefónica y entregar el código OTP al usuario. Cuando el usuario responde, el *Call Manager Server* entrega el código OTP durante el tiempo en que transcurre la llamada. Al finalizar la llamada, la App muestra una ventana para teclear el OTP. El usuario debe enviar el código OTP al *Login Server* para su validación.

Una vez recibido el código OPT, el *Login Server* verifica su validez comparándolo con el código OTP entregado por el *Data Base Server*, previamente. En caso de ser correcto, el *Login Server* solicita la huella dactilar del usuario.

- La tercera fase de autenticación inicia con la solicitud de la huella dactilar al usuario. Es importante mencionar que, las huellas dactilares son un rasgo en la fisionomía que no cambia con el tiempo; por lo tanto, se puede solicitar aleatoriamente un dedo de la mano para su validación.

  Una vez escaneado el dedo con el sensor de huella dactilar del teléfono celular, se genera una plantilla que se le aplica una función *fuzzy hashing* antes de ser enviada para contrastarla con otro *hash* del mismo tipo generado por parte del servidor.

Una vez verificado el *hash* recibido, el *Login Server* notifica al usuario sobre el proceso de validación. En caso de ser correcto, el usuario tiene acceso al sistema, y en caso contrario, se notifica sobre el error en el proceso de autenticación. El diagrama UML de la propuesta se presenta en la figura 3.

Análisis Informal Seguridad

Con la finalidad de sustentar la elección de los métodos de autenticación, se presenta un análisis por cada fase.

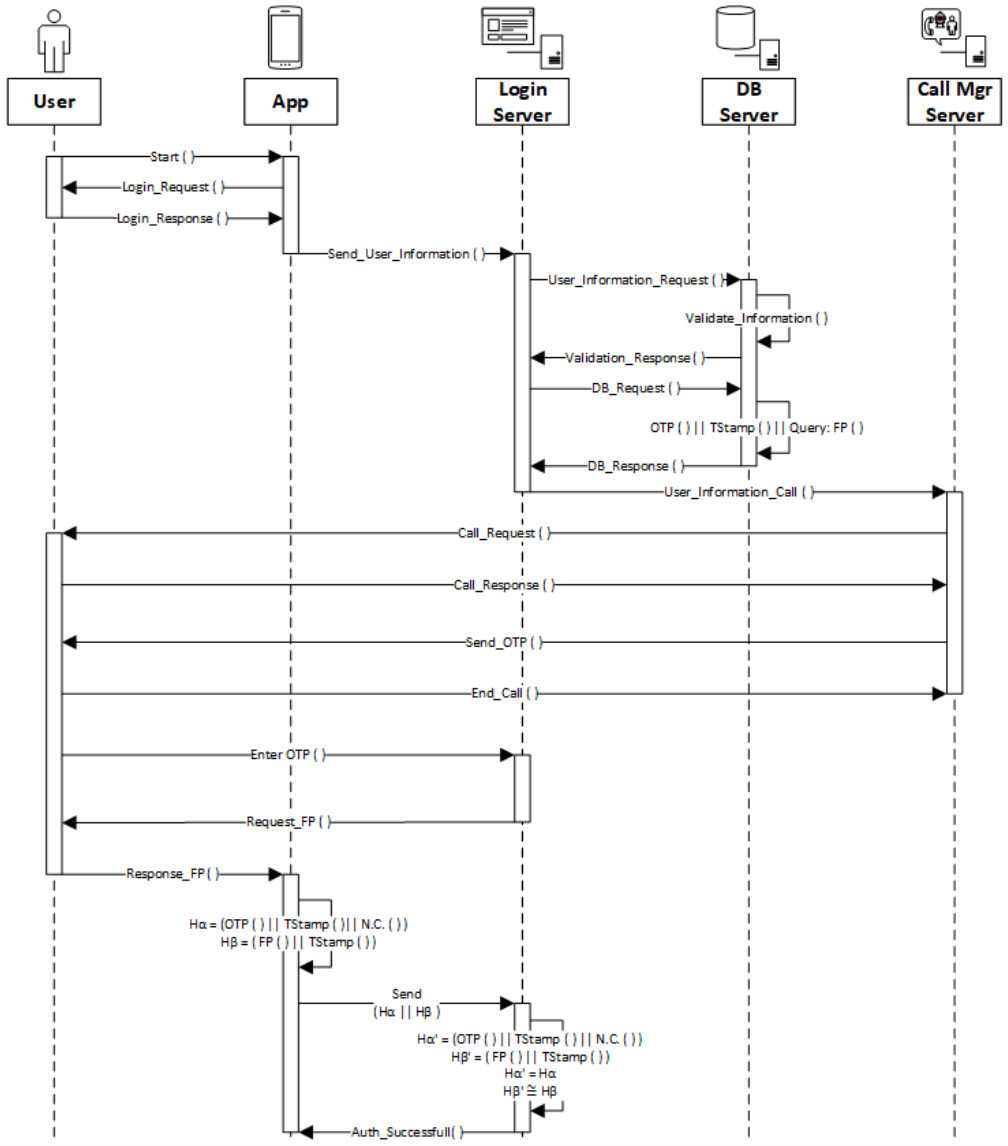


Figura 3 Diagrama de secuencia multifactor por Telelogin propuesto.

Análisis del Uso de *Image-Based Password*

El primer elemento de seguridad a utilizar en la propuesta, es un mecanismo de Image-Based Password. Se propone este sistema de autenticación basado en imágenes aleatorias porque es invulnerable a brute force attack, key loggers y shouder-surfing [Sosa, 2018]. Además, el usuario no podrá elegir una contraseña débil y le asumirá una mayor dificultad el divulgarla.

Al ser imágenes seleccionadas por el usuario en base a su gusto, se vuelve más fácil de recordar en lugar de memorizar contraseñas complejas [Dhamija, 2000]. El

Image-Based Password se convierte en una gran ventaja al momento de utilizar contraseña con baja frecuencia.

Análisis del Uso de *Bring Your Own Device* (BYOD)

Se describe como algo que se tiene y, en la propuesta, se utiliza como identificación principal del método el número telefónico usado por el usuario; sin embargo, al estar mezclado su uso con la aplicación instalada y un teléfono celular compatible, se complementa su uso con el concepto BYOD, lo que refuerza el mecanismo de seguridad SYH.

En este sentido, se entiende que el usuario mantiene más cerca su dispositivo móvil que otro dispositivo de autenticación, como puede un *token*, o tarjetas inteligentes.

Análisis Sobre la Realización de la Llamada

Una vez que el número telefónico ha sido verificado por el servidor de autenticación; el *Call Manager Server* realiza una llamada telefónica al usuario mediante el servicio de PSTN para comprobar que el teléfono esté siendo utilizado por el usuario y no exista un ataque *man-in-the-middle*. Se ha optado por que el servidor realice la llamada, en lugar del usuario, por los siguientes motivos:

- La inteligencia artificial del software en el *Call Manager*, tiene más probabilidades de ser susceptible a un ataque de ID *spoofing* telefónico que un usuario que espera una llamada *just* in time.
- El servidor *Call Manager* únicamente realiza llamadas si se cumplieron las condiciones de autenticación anteriores.
- En ningún caso el *Call Manager* acepta llamadas entrantes, por lo que la administración de las líneas se agiliza.
- El tiempo de la llamada no implica costo al usuario.

Análisis del Uso del Código OTP

Por el contrario del protocolo de Telelogin [Fujii, 2008] propuesto por Fujii en el que el usuario realiza una llamada telefónica al servidor del servicio remoto e introduce un NIP durante el proceso, en la propuesta de es el servidor Call Manager

la entidad que envía al usuario un OTP (haciendo uso de una red diferente a Internet como es la PSTN) durante una llamada telefónica. Las ventajas de seguridad existentes en esta mejora son:

- Un NIP pertenece al esquema de la contraseña tradicional, por lo cual, es difícil de recordar si no se usa con frecuencia.
- El OTP es generado por el mecanismo de autenticación, tiene un tiempo de vida limitado y sólo puede ser utilizado una vez.
- El usuario no envía una clave privada durante la llamada, sino que al ser él quien recibe el OTP, el proceso se vuelve resistente a un ataque de robo de información mediante *phishing* telefónico.

Análisis del Uso de Biometría por Huella Dactilar

El mecanismo de autenticación *SYA* se representa en algo que se es. Los rasgos biométricos de cada persona entran como identificación de este enfoque, por lo que en el protocolo de autenticación se hace uso de la huella dactilar por ser un rasgo biométrico único y, se pueden apreciar las siguientes ventajas:

- La huella dactilar no cambia durante el tiempo.
- El INE tiene registradas las huellas dactilares de los ciudadanos mexicanos.
- La mayoría de los teléfonos de gama media y alta cuentan con un sensor de huellas dactilares en el 2019 y el número aumentará en los próximos años.
- Es el factor de autenticación biométrica más utilizado en el mundo y por consecuencia el más conocido y aceptado por las personas.
- Es un método de identificación inapelable y con validez legal.
- Requiere menos recursos de procesamiento que otros sistemas como el escaneo de la retina o la palma de la mano.
- Es más seguro, no es susceptible a cambios en el ambiente y tiene una menor tasa de error que el reconocimiento facial o el reconocimiento de voz.

Análisis del Uso de un Sello de Tiempo

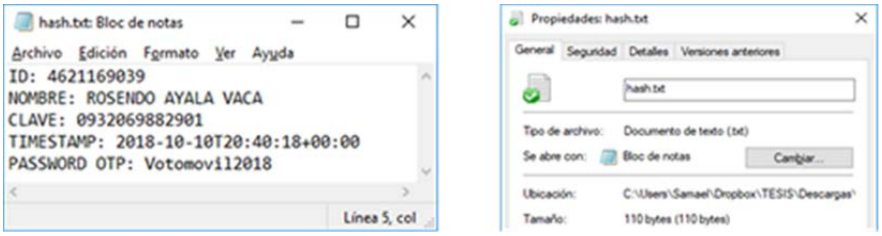
El proceso de autenticación, en el momento de enviar la información personal del dispositivo al servidor de autenticación, puede llevar una marca del tiempo; con este

sello de fecha y hora, se garantiza la integridad de que la operación se lleva a cabo en un determinado instante en el tiempo. Este sello concatenado a los demás parámetros a enviar vuelve imposible la reproducción de la operación en caso de que el canal de red fuera comprometido y dejará de ser seguro.

Análisis del Uso de una Función *hash* SHA2-512

Una función *hash* criptográfica es un algoritmo matemático que, con una entrada A, devuelve una salida B. La salida B generada del lado del cliente se compara contra B' almacenada del lado del servidor y de existir coincidencia se valida la identidad del usuario: B=B'. Es una buena práctica de seguridad nunca enviar información en texto sin cifrar, por lo que la propuesta incluye el envío de todos los elementos de identificación concatenados a autenticar en una cadena de tipo *hash* con la misma función *hash* de los elementos concatenados del lado del servidor.

En la figura 4a se muestra el archivo en formato txt que se utilizó para hacer pruebas de rendimiento de la función *hash*, y en la figura 4b se muestra el tamaño y formato del archivo. El archivo fue sometido a una comparación de funciones hash en el sitio web de criptografía Jit-Solutions desarrollado por [Ortega, 2018]. En la tabla 1, se muestran los tiempos de ejecución de cada función Hash aplicada al archivo hash.txt, así como, las cadenas cifradas.



a) Archivo con datos *b) Propiedades del archivo*

Figura 4 Prueba de cifrado de archivo.

Tabla 1 Comparativa de tiempos de ejecución de distintas funciones *hash*.

Función Hash	Tiempo de ejecución	Cadena cifrada
SHA2-256	1ms	caedfe31086af5981e62fbb45dd4ed7ccb0122f07993493ff2d4821610b17e94
SHA2-512	1 ms	82cebf821a09f60dc1bca2dd32d989b6d78e31a3c6654c6751e6ea09b9e1bf5059457b30bbf640f9afb3458ca22e6875f3bafeee4e3a4a73f7f95be9e06b4424
SHA3-512	4 ms	f23cdf85a40cb804253eda27e9ecd8e4effa3373f3839f191d07c3bcf4efc3706be8a4d34d9b0fa724a2c7229c18138713f27f56b33cd19896df3c23f586acdc

Análisis del Uso de una Función *hash fuzzy hashing*

No todos los puntos a analizar durante el proceso de autenticación van a ser siempre exactos y, el caso de la identificación biométrica, es un ejemplo. A diferencia de la función SHA-2, un algoritmo criptográfico de *fuzzy hashing* no tiene un cambio radical en su cadena de salida por un cambio tan imperceptible como un byte. El *fuzzy hashing* permite evaluar si existen cadenas con estructuras similares que contengan un porcentaje de similitud con el *hash* original (A'≅B^'), lo que vuelve a esta función más eficiente cuando se esperan cambios aceptables entre la cadena de salida y la cadena a comparar en el servidor y conserva cifrada la información transmitida. Los cambios esperados del *hash* A' en el teléfono móvil con el *hash* B' almacenado en el servidor de base de datos se deben a las posibles permutaciones al momento de posicionar el dedo, sensor sucio, falta de precisión o daños accidentales en las huellas dactilares causadas por ligeras cortaduras y quemaduras que afecten los arcos, remolinos y minucias. Un sistema de autenticación de huellas dactilares no compara imágenes idénticas, sino realiza una comparación de las minucias y la posición relativa entre ellas. En la tabla 2, se muestran los cambios entre cadenas de texto como ejemplo del funcionamiento de *Fuzzy Hashing* [OI, 2017] y sus respectivas permutaciones a los *Hashes* obtenidos entre versiones diferentes de la imagen en color rojo. El campo de porcentaje aplica para el nivel de coincidencia entre la huella original y la huella consultada para el *Hash* propuesto en el factor de biometría.

4. Discusión

Se ha presentado el análisis a dos propuestas realizadas por Haruko Fujii en 2008 y 2013, evidenciando vulnerabilidades de seguridad y áreas de mejora. A partir de ese análisis de seguridad, se ha propuesto un nuevo mecanismo de autenticación de dos vías y tres factores. Las dos vías hacen referencia a los medios de comunicación que utiliza el usuario para ser autenticado, que son la red IP y PSTN. Por otra parte, los tres factores hacen referencia al uso de los tres paradigmas *SYH*, *SYK* y *SYA*, que son empleados en las tres fases descritas previamente.

Tabla 2 Comparativa de resultados entre función *hash512* y *fuzzy hash*.

Huella Dactilar	Descripción	% Coincidencia
 **Figura** 1**. Variante 8 de huella dactilar.**	Ejemplo de simulación 8 de huella consultada donde se observa un ligero cambio en los arcos, intersecciones y remolinos en el área central de la huella dactilar.	**88.75%**
	SHA-512 4203134AFB28D5AD68B1165A1CD54C38886EC7DF5BE5421 4A1B0B7506796D77BC074CA3A61DCB38282DE463A48744C 1DC5A06B401BB10EFE33F87422B2174B2D	
	Fuzzy-Hash uYtJTFrA6zex9ozD5T4MjiS4uFnDuS+4dZ/+qgJZj1Am9xIqd2U6Zf:9JTFK oz1esDiGTGAmFQH	
 **Figura** 2**. Variante 12 de huella dactilar.**	Ejemplo de simulación 12 de huella consultada donde se observan cuatro cambios contiguos en la zona superior de la imagen afectando arcos, intersecciones y remolinos.	90%
	SHA-512 4F0ED4FC6D6DA187A2A794BCC71886756C43B6C2AC67E13 1A1CF8B7643E64F3F3E7C8945C00169FC94F8ACEA1549775 BEFE816D6A40A8C2B0FB512A38A36CFF4	
	Fuzzy-Hash uYtJTFrA6zex9ozD5T4MjiSoHFnDuS+4OsivqgJZj1Am96I/YIP6Zf:9JTFKoz 1eNDiufGAmbxM	

Es importante mencionar que, se mantiene la idea original de Haruko Fujii en la nueva propuesta, y los cambios propuestos no afectan su eficiencia. En particular, el uso de la huella dactilar es más aceptado por usuarios y tiene menos errores que la autenticación por voz. Además, el uso de la voz en un entorno abierto, donde se encuentra contaminado por ruidos externos, puede dificultar la autenticación.

También se ha presentado el método de fuzzy hash como una buena solución para verificar la legitimidad de la huella dactilar en la tabla 2. En este punto, se debe considerar el nivel de coincidencia que se requiere para aceptar la solicitud de autenticación. En la tabla 2, se han presentado dos ejemplos. El primero hace referencia a un porcentaje de coincidencia del 88.75%, mientras que, el segundo hace referencia a un porcentaje del 90%. La propuesta considera cualquiera de estos dos porcentajes debido a que obtener el 100% de coincidencia ocasionaría varios rechazos.

La elección de la función hash se encuentra evidente en los resultados presentados en la tabla 1 donde el tiempo de ejecución de la función sha2-512 es menor que el tiempo de ejecución de la función sha3-512, y mantiene una seguridad equiparable.

Un cambio significativo es el cambio método en el paradigma *SYK* donde se ha cambiado la necesidad de memorizar una contraseña compleja por recordar tres imágenes.

5. Conclusiones

Se ha realizado un análisis a dos propuestas de Telelogin presentadas en [Fujii, 2008] y [Fujii, 2013]. Los trabajos han servido para conocer las medidas de seguridad empleadas y poder identificar áreas de oportunidad. Por lo tanto, a partir de dichos trabajos, se ha propuesto un nuevo mecanismo de autenticación en dos vías y tres factores de autenticación.

La propuesta incluye un reto basado en imágenes que cambia el paradigma de memorizar por recordar, haciendo más fácil el proceso para los usuarios que tener que memorizar contraseñas complejas. También se incluye el uso de un dispositivo personal, el teléfono inteligente, como medida de seguridad, y particularmente, el número telefónico que es utilizado para recibir la llamada telefónica. Además, se incluye el uso de la huella dactilar como método de autenticación debido a que varios teléfonos inteligentes incluyen un lector.

Los análisis realizados a cada método de seguridad evidencian que la propuesta es segura y se encuentra orientada a los entornos de desarrollo de aplicaciones móviles debido a que son los sistemas más utilizados.

Como trabajo futuro, se encuentra en desarrollo un modelado y simulación en BPMN con Bizagi para conocer el porcentaje de tiempo estimado en completar el proceso de autenticación y conocer el número de intentos fallidos.

6. Bibliografía y Referencias

[1] Allan, D. Microsoft’s sharper speech recognition tech should supercharge Cortana, Future Publishing Limited Quay House, 2017.

[2] Ayala-Vaca, R. Autenticación Multi-factor para reducir los riesgos de seguridad, Tecnotrend, vol. 5, p. 54, 2018.

[3] Dhamija, R. y Perrig, A. Deja Vu: A User Study Using Images for Authentication, USENIX Security Symposium, 2000.

[4] CONDUSEF, Spoofing, Proteja su dinero, no. 220, pp. 22-24, 2018.

[5] CSID, Consumer Survey: Password Habits. A study of password habits among American consumers, 2012.

[6] De Saint-Exupéry, A. El Principito, México: Diana, 1956.

[7] Dong-Ju, K., Kwang-Woo, C., Kwang-Seok, H. Person authentication using face, teeth and voice modalities for mobile device security. IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2678-2685, 2010.

[8] Fujii, H., Shigematsu, N., Kurokawa, H., and Nakagawa, T. Telelogin: a two-factor two-path authentication technique using caller ID. NTT Techincal Review, vol. 6, no. 8, 2008.

[9] Fujii H., Tsuruoka Y. Three-Factor User Authentication Method Using Biometrics Challenge Response. Financial Cryptography and Data Security, vol. 7859, 2013.

[10] Guccione, D. What the Most Common Passwords of 2016 List Reveals, 2017.

[11] Kinnunen, T., Zhizheng, W., Kong, A.L., Filip, S., Eng, S.C., Haizhou, L. Vulnerability of Speaker Verification Systems Against Voice Conversion Spoofing Attacks: the Case of Telephone Speech. IEEE International Conference on Acoustics, Speech and Signal Processing, 2012.

[12] Martinez-Pelaez, R., Pomykała, J., Rico-Novella, F., Satizabal, C. Using fingerprint biometric-based identification on tables of poker and blackjack to enhance the security in casinos. Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, 2011.

[13] OI, T. ssdeep - fuzzy hashing program, SSDEEP Project, 2017.

[14] Ortega García, F. Diseño de un mecanismo para firmado múltiple de documentos digitales., Leon: Universidad De La Salle Bajio, 2018.

[15] Pastorino, C. Estadísticas y reglas para predecir contraseñas: ¿es obsoleta la fuerza bruta?, 2017.

[16] Schneier, B. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth). Jhon Wiley & Sons, Inc. 1996.

[17] Piotrowski, Z., Gajewski, P. Voice spoofing as an impersonation attack and the way of protection. Journal of Information Assurance and Security, vol. 2,

pp. 223-225, 2007.

Rhodes, M. Information Security The Complete Reference, McGraw-Hill, 2013.

[18] Sosa-Valles, P., Villalobos-Serrano, J. G., Velarde-Alvarado, P., García, V., Parra-Michel, J. R., Mena, L., y Martínez-Peláez, R. My Personal Images as My Graphical Contraseña, IEEE Latin America Transactions, vol. 16, no. 5, pp. 1516-1523, 2018.

[19] Velásquez, I. Caro, A., Rodríguez, A. Authentication schemes and methods: A systematic literature review. Information and Software Technology, vol. 94, pp. 30-37, 2018.

[20] Zahid, H., Khan, U. Comparative Study of Authentication Techniques. International Journal of Video & Image Processing and Network Security, vol. 10. no. 4, pp. 9-13, 2010.