My Personal Images as My Graphical Password

P. A. Sosa-Valles, J. G. Villalobos-Serrano, P. Velarde-Alvarado, V. García, J. R. Parra-Michel, L. Mena, R. Martínez-Peláez

***Abstract*— In 1996, Blonder introduced the first authentication system based on a graphical password. Since then, researchers have proposed several systems in the literature enhancing security properties to prevent brute-force, guessing, and shoulder-surfing attacks. However, many systems were developed using impersonal images, hindering their identification and retention. As a solution, Takada-Toike, and Herzberg-Margulies introduced systems using personal images in 2002 and 2012, respectively. Nonetheless, users require passing many stages during the authentication phase, making the systems unsecured. As a solution, we propose a system where each user creates a graphical personal password and needs to pass a stage. Security analysis demonstrates that the proposal can resist very well-known attacks, making it secure and useful for web services.**

***Keywords*— authentication; electronic services; image-based; observation; usable security.**

I. INTRODUCCIÓN

EL NÚMERO de cuentas crece día a día debido a la gran variedad de servicios electrónicos y a las alternativas de conectividad. En consecuencia, los usuarios de Internet deben recordar varias contraseñas alfanuméricas, tales como un número personal de identificación (NIP) o contraseña. De acuerdo a Florencio y Herley [8], y a un estudio realizado por los autores, los usuarios con más de 20 cuentas utilizan entre 5 y 7 contraseñas, con una longitud de 7 caracteres en promedio, seleccionado contraseñas simples o débiles [11].

Las contraseñas simples se pueden generar a partir de una palabra semilla que sirve para generar contraseñas; es decir, los usuarios suelen cambiar una letra por un número, utilizar letras en mayúscula y crear combinaciones para definir varias contraseñas. Para incrementar la seguridad en las contraseñas, se pueden utilizar generadores de contraseñas complejas que incluyen una longitud de 10 o más caracteres, y se encuentra formada por números, letras y caracteres especiales.

P. A. Sosa Valles, Universidad Autónoma de Ciudad Juárez, Ciudad Juárez, Chihuahua, México, al115044@alumnos.uacj.mx

J. G. Villalobos Serrano, Universidad Autónoma de Ciudad Juárez, Ciudad Juárez, Chihuahua, México, al115000@alumnos.uacj.mx

P. Velarde Alvarado, Universidad Autónoma de Nayarit, Tepic, Nayarit, México, pvelarde@uan.edu.mx

V. García, Universidad Autónoma de Ciudad Juárez, Ciudad Juárez, Chihuahua, México, vicente.jimenez@uacj.mx

J. R. Parra Michel, Universidad de la Salle Bajío, León, Guanajuato, jrparra@delasalle.edu.mx

L. Mena, Universidad Politécnica de Sinaloa, Mazatlán, Sinaloa, México, lmena@upsin.edu.mx

R. Martínez Peláez, Universidad De La Salle Bajío, León, Guanajuato, México, rmartinezp@delasalle.edu.mx

Corresponding author: *Rafael Martínez Peláez*

Sin embargo, el esfuerzo que requiere el usuario para recordar una contraseña de 10 o más caracteres es alto, dificultando el proceso de autenticación debido a las limitaciones del cerebro humano para recordar secuencias complejas [3], [14] y [24].

Con la intención de ofrecer un sistema de autenticación con menor requerimiento de esfuerzo a las personas, en términos de memoria, Blonder introdujo un método de autenticación basado en imágenes [5]. La propuesta de Blonder se fundamenta en los siguientes trabajos [2], [9], [18] donde se demuestra que el proceso de reconocer requiere menor esfuerzo que el proceso de recordar.

A partir del trabajo de Blonder, se han propuesto varios sistemas de autenticación [1], [6], [7], [10], [12], [13], [15], [17], [19], [21], [22], permitiendo definir tres categorías [4]:

(i) sistemas basados en recordar (*recall-based*) – *drawmetric*: se refiere a la capacidad del ser humano de acordarse de un evento, pieza de información, o imagen.

(ii) sistemas basados en reconocer (*recognition-based*) – *cognometric*: se refiere a la capacidad del ser humano de identificar un evento, pieza de información, o imagen.

(iii) sistemas basados en señales para recordar (*cued-recall based*) – *locimetric*: se refiere a la capacidad del ser humano de acordarse de un evento, pieza de información, o imagen utilizando señales o pistas

La principal diferencia entre los procesos de recordar – sin ayuda – y recordar utilizando señales es que la señal o pista se relaciona con la información que se recuerda, ayudando en el proceso de recuperación de la memoria. Por otra parte, el proceso de reconocer requiere menor esfuerzo porque involucra pistas que activan la información relacionada en la memoria [2] y [18].

A partir de la clasificación presentada previamente, y de las ventajas que ofrecen los sistemas basados en reconocimiento, se propone un sistema basado en imágenes personales. Al igual que las propuestas [10] y [21], el sistema presentado requiere de imágenes personales para crear una contraseña gráfica. Las contribuciones que se presentan son dos. La primera contribución es el proceso de creación de una contraseña gráfica personal, utilizando imágenes personales del usuario y seleccionando su longitud entre 4 y 10 opciones. La selección de imágenes considera la utilización de imágenes almacenadas en cualquier dispositivo de almacenamiento o tomar una fotografía a través de una cámara web. La segunda contribución es el proceso de autenticación con dos retos personalizados. Los retos que se pueden utilizar son: agregar imágenes ruido o desplazamiento aleatorio de imágenes. Además, se realiza un

análisis de seguridad demostrando que la propuesta es segura contra ataques posibles en el mundo real.

A continuación, se presenta la estructura del artículo. Los trabajos relacionados que fundamentan la propuesta son descritos en la sección II. En la sección III, se describe el diseño del sistema donde se definen las fases y entidades. El desarrollo del sistema se explica en la sección IV. La evaluación de seguridad se explica en la sección V. Finalmente, las conclusiones son presentadas en la sección VI.

II. TRABAJOS RELACIONADOS

La presente sección tiene la finalidad de mostrar una visión general de las propuestas más significativas en el tema, en orden cronológico. Se destacan los procesos de registro y autenticación de cada propuesta.

En 1996, Blonder [5] propuso un sistema de autenticación basado en una contraseña gráfica. En este sistema, el usuario debe tocar ciertas áreas predeterminadas de una imagen y en una secuencia especifica. El autor argumento que, las contraseñas textuales son difíciles de recordar para los usuarios, y en particular las contraseñas alfanuméricas fuertes.

En 1999, Jermyn *et al.* presentaron un sistema de contraseña gráfica llamado *draw-a-secret* (DAS) [13]. En este sistema, el usuario debe dibujar una imagen dentro de una cuadrícula rectangular de medidas $G \times G$. La cuadrícula contiene n celdas donde sus coordenadas son dadas por $(x, y) \in [1 \dots G] \times [1 \dots G]$. En el proceso de registro, la imagen dibujada en la cuadrícula sirve para generar la secuencia de coordenadas que formaran la contraseña. Como resultado, la longitud de la contraseña es la suma de las coordenadas de las secuencias de desplazamiento de cada componente de la imagen. En el proceso de autenticación, el usuario debe dibujar la misma imagen dentro de los mismos cuadros.

En 2000, Dhamija y Perrig introdujeron el sistema Déjà Vu [6]. Este sistema hace uso de la galería de arte aleatorio de Andrej Bauer. En el proceso de registro, el servidor muestra un conjunto de n imágenes de la galería de Andrej Bauer al usuario. El usuario debe elegir p imágenes con el objetivo de crear un portafolio personalizado. En el proceso de autenticación, el sistema lanza un desafío al usuario, mostrando un conjunto de m imágenes que contienen algunas imágenes almacenadas en el portafolio personal. El usuario debe seleccionar las imágenes correctas.

En 2003, Takada y Koike desarrollaron el sistema Awase-E [21]. En este sistema, el usuario tiene la posibilidad de utilizar imágenes personales. En el proceso de registro, el usuario debe escoger imágenes personales y almacenarlas en el sistema. En el proceso de autenticación, el sistema lanza un desafío de cuatro etapas, mostrando nueve imágenes y solo una imagen será de las seleccionadas por el usuario, o en otros casos no se mostrarán imágenes y el usuario deberá indicar "*No pass-image*". El usuario debe pasar las cuatro etapas correctamente.

En 2005, se lanzó al mercado la aplicación Passfaces de la empresa Passfaces Corporation [17]. El sistema muestra una matriz de 3x3 con caras de personas que el usuario debe seleccionar para establecer una contraseña. En el proceso de registro, el usuario debe seleccionar una cara de las nueve presentadas en tres etapas diferentes, generando su contraseña personal. En el proceso de autenticación, se presentan cuatro desafíos que consisten en presentar 9 fotografías y solo una es correcta, en cada reto.

En el mismo año, se publicó la propuesta PassPoints [22] inspirado en el trabajo de Blonder. Los autores realizaron dos mejoras desde la perspectiva del usuario: 1) el click no debe ser en la posición exacta, dejando un margen de hasta .25cm y 2) los usuarios pueden elegir cualquier área de la imagen. Además, la contraseña no se almacena en claro, sino el resultado de una función hash. El usuario debe elegir cinco puntos dentro de una imagen para crear la contraseña.

En 2012, Herzberg y Margulies propusieron un sistema basado en imágenes personales que consta de dos versiones [10]. En el *single stage*, el sistema muestra un pequeño conjunto de imágenes L y solo una imagen k pertenece al conjunto de imágenes seleccionadas por el usuario. En cada inicio de sesión, el conjunto de imágenes L se cambia de manera aleatoria, pero permanece la imagen k. En el *multiple stages*, el sistema muestra n etapas donde cada etapa presenta un pequeño conjunto de imágenes L y solo una imagen k pertenece al conjunto de imágenes seleccionadas por el usuario. Cabe mencionar que, el conjunto de imágenes L y la imagen k aparecen siempre en la misma etapa para evitar que un atacante pueda identificar la imagen correcta.

III. DISEÑO DEL SISTEMA

El presente sistema de autenticación se inspira en la propuesta de Takada y Koike [21], quienes utilizaron fotografías personales para construir una contraseña gráfica.

El sistema propuesto consta de seis fases:

(i) registro, el usuario crea una cuenta en el sistema web para ser miembro de la comunidad.
(ii) selección de imágenes, el usuario define el número total de imágenes personales, y posteriormente, el usuario debe elegir las imágenes – fotografías, dibujos, etc. – para formar su portafolio.
(iii) definición de secuencia de imágenes, el usuario elige la secuencia que dará origen a la contraseña gráfica a partir de las imágenes almacenadas en su portafolio.
(iv) inicio de sesión, el usuario solicita acceder a su cuenta.
(v) autenticación, el usuario debe superar el desafió para demostrar que es el legítimo propietario de la cuenta.
(vi) cambio de contraseña, el usuario tiene la posibilidad de cambiar las imágenes y secuencia cuando se requiera.

A. Entidades del sistema

Las entidades del sistema son:

- El usuario es quien debe crear una cuenta y una contraseña gráfica a partir de la selección de imágenes personales.
- El sitio web tiene la función de validar y almacenar la información recibida del usuario. Además, se encarga de establecer el puente entre el usuario y el servicio creación de contraseña.

- El servicio creación de contraseña se encarga de gestionar las imágenes para establecer la contraseña gráfica definida por el usuario.
- El servicio autenticación tiene tres funciones. La primera función verificar la existencia del usuario en el sistema. La segunda función es generar el desafío-respuesta que debe superar el usuario. La última función es validar la respuesta enviada por el usuario.

B. Fase de registro

El usuario puede iniciar la fase de registro desde cualquier lugar y en cualquier momento a través de su navegador web. En el proceso de registro, el usuario comparte su información personal con el sistema web a través de un formulario de registro. En caso de cumplir con todos los requisitos del formulario de registro, la información es almacenada en una base de datos y se inicia la siguiente fase.

C. Fase de selección de imágenes

Inicialmente, se procede a llamar al servicio creación de contraseña, que es el proceso mediante el cual se seleccionan las imágenes personales.

El usuario requiere realizar las siguientes actividades:

(i) Selección del número de imágenes personales, el sistema brinda la opción al usuario de elegir entre 4 y 10 imágenes para crear su portafolio de L imágenes.

(ii) Selección de imágenes que desea utilizar el usuario, el sistema permite activar y utilizar la cámara web de una laptop o de una computadora para capturar imágenes en el momento. Además, se pueden utilizar imágenes guardas en el disco duro o dispositivo de almacenamiento externo.

(iii) Guardar cada imagen seleccionada en la base de datos.

Una vez almacenadas las imágenes, se inicia la siguiente fase.

D. Definición de secuencia de imágenes

La Fig. 1 muestra a través de un diagrama de secuencia en UML (*Unified Modeling Language*) las fases de registro, selección de imágenes y creación de contraseña gráfica personal.

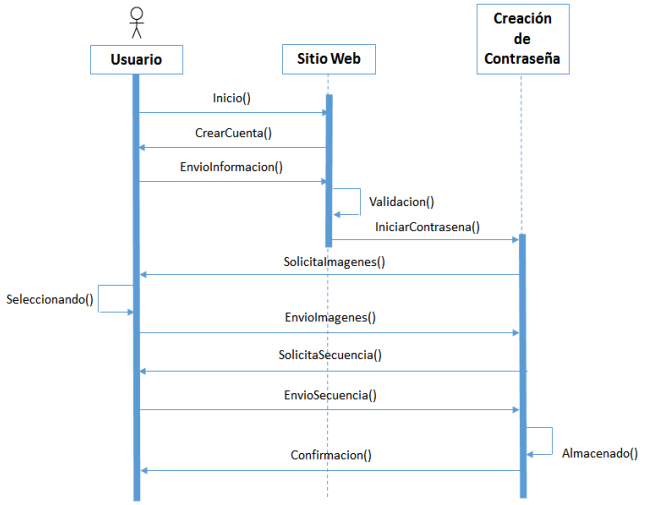


Figura 1. Fases para crear la contraseña personal.

El servicio creación de contraseña es el proceso mediante el cual se define la secuencia de imágenes personales para crear la contraseña gráfica.

El usuario debe definir la secuencia que dará origen a la contraseña gráfica. Es importante mencionar que, la secuencia no permite seleccionar dos veces la misma imagen. Por lo tanto, se tiene $n!$ combinaciones posibles.

Una vez seleccionada la secuencia de imágenes, se guarda la contraseña en la base de datos y se confirma al usuario.

En este punto, se ha creado una contraseña gráfica utilizando imágenes personales.

E. Inicio de sesión

El usuario requiere acceder al sitio web para realizar alguna transacción. En respuesta, el sitio web solicita el identificador de la cuenta (p. ej. nombre o seudónimo). El usuario debe introducir y enviar su identificador. Una vez recibido el identificador, se procede a verificar su existencia en la base de datos. En caso de ser positivo, se inicia la fase de autenticación.

F. Autenticación

La fase de autenticación presenta uno de los siguientes desafíos: a) presentar imágenes de manera aleatoria y/o b) agregar imágenes *ruido*.

Una vez presentado el desafío, el usuario debe responder y enviar su respuesta. El sistema de autenticación verifica la respuesta y notifica el estatus al usuario – autenticación correcta o autenticación incorrecta. En la Fig. 2, se describe el procedimiento de autenticación.

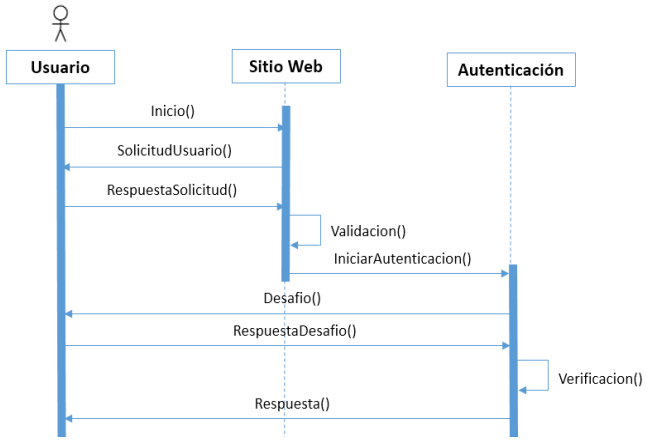


Figura 2. Fases del sistema de autenticación.

G. Cambio de contraseña

Uno de los principales requisitos para los usuarios es la posibilidad de cambiar su contraseña cuando lo requieran. Por lo tanto, el presente sistema de autenticación permite a los usuarios cambiar su contraseña por medio de modificar la secuencia.

El usuario debe presionar el botón “Cambiar contraseña” y después de ser autenticado puede realizar la actualización de la secuencia para generar una nueva contraseña.

H. Medidas de seguridad

Se han implementado las siguientes medidas de seguridad, en caso de detectar un ataque de seguridad: 1) bloquear la cuenta de usuario 24 horas, cuando se reciban tres fallas en el proceso de autenticación; y 2) notificar vía correo electrónico al propietario de la cuenta informando sobre el intento de acceso fallido, cuando se reciban tres fallas en el proceso de autenticación.

IV. DESARROLLO DEL SISTEMA

En la presente sección, se describe el desarrollo del prototipo del sistema. El prototipo fue desarrollado utilizando Java y el gestor de base de datos es PhpMyAdmin. Se utilizaron dos equipos de cómputo en el desarrollo. El primer equipo consta de 6 GB en memoria RAM, procesador AMD A6-5200 de cuatro núcleos y con una velocidad de 2.0 GHz. El segundo equipo consta de 16 GB en memoria RAM, procesador AMD A8-6410 de cuatro núcleos y con una velocidad de 2.0 GHz. En ambos casos, se utilizó NetBeans IDE 8.2.

A. Suposiciones iniciales

Se tienen las siguientes suposiciones:

- Se utiliza certificados digitales y el protocolo *Secure Sockets Layer version* 3 (SSLv3) para establecer una conexión segura entre el equipo del usuario y el servidor web.
- Se tiene una cámara web instalada en el equipo del usuario para tomar fotografías.
- Se tiene instalada en el equipo del usuario la versión 8 o superior de Java.

B. Primera fase: creación de contraseña gráfica personal

Inicialmente, el usuario debe completar la fase de registro con su información personal y posterior a su validación, la información es almacenada en la base de datos.

Después, se inicializa la fase de selección de imágenes donde el usuario definirá el número de imágenes que utilizará para crear su contraseña. El número de opciones se encuentra entre 4 y 10. En la Fig. 3, se muestra el mensaje que recibe el usuario.

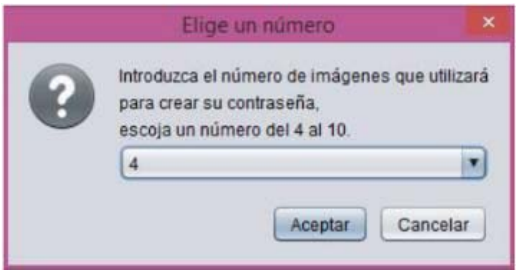


Figura 3. Selección del número de imágenes para crear la contraseña personal.

Una vez seleccionado el número de imágenes, el usuario debe elegir las imágenes. El código que se programó para encender y conectar la cámara web con el sistema se presenta en la Fig. 4. El código permite encender la cámara web interna o externa conectada en cualquier equipo de cómputo sin necesidad de instalar controladores adicionales. Además, el código soporta múltiples plataformas – Windows, Mac Os, Linux - y arquitecturas de 32 bits y 64 bits.

```
public void gui()
{
    JPanel pnlCamara = new JPanel();
    webcam.setViewSize(WebcamResolution.VGA.getSize());
    WebcamPanel panel = new WebcamPanel(webcam);
    panel.setMirrored(false);
    panel.setFPSDisplayed(false);


    pnlCamara.add(panel);
    tomar_fotos.this.add(pnlCamara);
    tomar_fotos.this.setResizable(false);
    tomar_fotos.this.pack();

}
```

Figura 4. Código para encender y conectar la cámara web.

El código que se muestra en la Fig. 4 define el tamaño del Jframe que se muestra en la Fig. 5.

Figura 5. Jframe para seleccionar y guardar imágenes.

A partir del Jframe que se muestra en la Fig. 5, el usuario puede tomar una fotografía o escoger una imagen desde la computadora para generar su portafolio de *L* imágenes. En caso de que, el usuario desee tomar una fotografía debe presionar el botón “Tomar Foto” y se capturará la imagen que aparezca en el recuadro del Jframe. Además, el usuario puede utilizar cualquier imagen que se encuentre en un disco duro a través del botón “Escoger imagen desde PC” (ver Fig. 6).

Figura 6. Cuadro de selección de imágenes en disco duro.

El usuario debe presionar el botón “Guardar cambios” para almacenar cada imagen seleccionada. La imagen se guarda con extensión JPG, y el nombre se genera de manera aleatoria y única. Por lo tanto, en la base de datos se tiene como ID el nombre de la imagen.

El resultado del proceso de selección y guardado de imágenes se muestra en la Fig. 7.

En este punto, el usuario ha seleccionado y guardado las imágenes, pero no se ha creado la contraseña. Por lo tanto, el usuario debe completar la fase de definición de secuencia de imágenes.

La Fig. 8 muestra el proceso de selección de imágenes, bloqueándose las imágenes seleccionadas para impedir su repetición. Al finalizar la secuencia, el usuario debe presionar el botón “Guardar Contraseña” para almacenar la secuencia en la base de datos.

Figura 7. Ejemplo de cuatro imágenes personales seleccionadas y almacenadas.

Figura 8. Ejemplo de selección de secuencia para crear la contraseña.

C. Segunda fase: autenticación

El usuario debe comenzar con la fase de inicio de sesión desde cualquier lugar y en cualquier momento a través de su navegador web. El sitio web solicita el identificador de la cuenta (p. ej. nombre o seudónimo). En respuesta, el usuario debe enviar el identificador a través de un canal de comunicación seguro.

Una vez recibido el identificador del usuario, el servicio autenticación se encarga de verificar la existencia del identificador de la cuenta en la base de datos. En caso de no encontrar alguna coincidencia, se emite una respuesta de error al usuario. En caso contrario, se procede a iniciar la fase de autenticación.

El usuario debe superar la fase de autenticación demostrando reconocer la secuencia que forma la contraseña. El servicio autenticación se encarga de generar un arreglo y a través de la función *Java Random*, las imágenes se presentan al usuario de manera aleatorio. La Fig. 9 muestra un fragmento del código utilizado para crear el desafió de presentar imágenes de manera aleatoria.

```
int index;
String temp;
Random random = new Random();
for (int i = arreglo.length - 1; i >= 0; i--)
{
    index = random.nextInt(i + 1);
    temp = arreglo[index];
    arreglo[index] = arreglo[i];
    arreglo[i] = temp;

    temp = arregloNombreFotos[index];
    arregloNombreFotos[index] = arregloNombreFotos[i];
    arregloNombreFotos[i] = temp;
    //System.out.println(index+"index+indice"+i);

}
```

Figura 9. Código de arreglo y desplazamiento aleatorio.

La Fig. 10 muestra un ejemplo del desafío “presentar imágenes de manera aleatoria” y como la posición de las imágenes cambia en cada inicio de sesión.

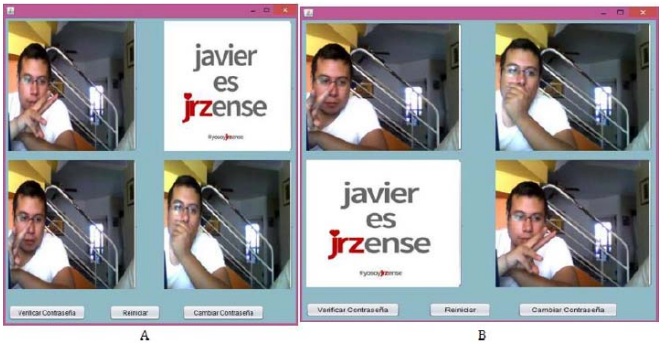


Figura 10. Ejemplo del desafío en la fase de autenticación.

En la Fig. 11 se muestra un ejemplo del desafío “agregar imágenes *ruido*”. Cabe mencionar que, el número de imágenes ruido se agregan de manera aleatoria y son proporcionadas por el sistema. Sin embargo, el número máximo de imágenes presentadas es de 10; por lo tanto, cuando un usuario utiliza 9 imágenes se podrá presentar una sola imagen ruido.

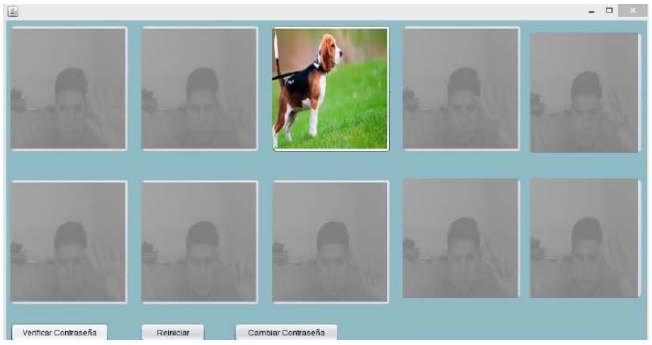


Figura 11. Ejemplo del desafío en la fase de autenticación.

Una vez que, el usuario ha finalizado de marcar las imágenes, se envía la secuencia generada al servicio autenticación para validar los valores. En caso de que la secuencia se encuentre en el orden esperado, se notifica al usuario.

V. EVALUACIÓN DE SEGURIDAD

En la presente sección, se describen las pruebas de seguridad realizadas al sistema para demostrar que es resistente a los ataques de *shoulder-surfing*, *brute-force* y *keylooger*. Las

propuestas [16], [20], [23] tienen como objetivo evitar el ataque de *shoulder-surfing*; sin embargo, el presente trabajo incluye dos ataques adicionales que se pueden utilizar en el mundo real para obtener la contraseña de la víctima. En cada prueba, la presente propuesta resiste al ataque, dificultando que un atacante pueda conocer la contraseña del usuario.

A. Ataque por keylogger

El *keylogger* es una herramienta que registra y almacena los eventos generados por el teclado y mouse, y posteriormente son consultados por el atacante. Debido a que todo usuario debe teclear su contraseña o presionar un botón se puede almacenar esa información antes de ser cifrada; es decir, la herramienta *keylogger* es un ataque pasivo que permite registrar todo evento generado por el teclado o mouse. El *keylogger* utilizado en la evaluación se llama "*keylogger-remoto*" y permite monitorear toda actividad a través de cualquier navegador web.

La prueba se realizó tres veces, utilizando una computadora diferente en cada ocasión con sistema operativo Microsoft Windows 7. Antes de llevar a cabo la prueba, se explicó a cada participante el funcionamiento del sistema de autenticación y se informó sobre la instalación de la herramienta con objeto de no invadir su privacidad y enfocarnos en los procesos de inicio de sesión y autenticación.

En la Fig. 12, se muestra el resultado del monitoreo realizado sin encontrar evidencia alguna sobre la secuencia de la contraseña gráfica personal. El resultado fue el mismo en cada prueba. Cabe mencionar que, el identificador de la cuenta es registrado por el *keylogger* debido a que se utiliza el teclado. Sin embargo, se evita registrar la contraseña y por lo tanto se resiste al ataque.

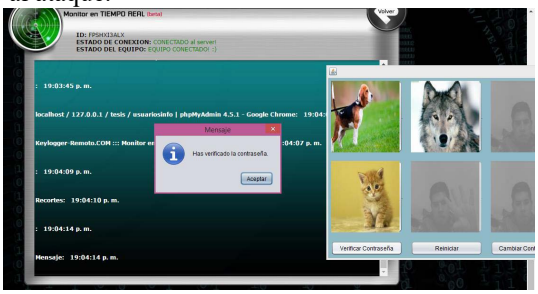


Figura 12. Resistente al ataque de *keylogger*.

B. Ataque por brute-force

El ataque de fuerza bruta o *brute-force* es un método mediante el cual un atacante prueba las posibles combinaciones de caracteres (número, letras, símbolos especiales) o imágenes hasta encontrar la secuencia correcta, que en este caso sería la contraseña.

La condición inicial fue deshabilitar la opción de bloqueo de la cuenta con la intención de agilizar la evaluación. Se solicitó a un participante crear una contraseña con las características deseadas. El participante eligió una longitud de 6 imágenes y cada imagen fue seleccionada personalmente. A partir de ese punto, el participante con el rol de atacante procedió a realizar el ataque de fuerza bruta para encontrar la contraseña. La prueba duró una hora y dio la posibilidad de realizar 123 intentos, sin encontrar la secuencia correcta.

En base al número de intentos y con la medida de seguridad de bloque (ver subsección III.H), el atacante hubiera tenido 41 bloqueos en base a $B = i/3$, donde B es el número de bloqueos, i es el número de intentos, y 3 umbral de intentos fallidos para iniciar bloqueo de 24 horas. Por lo tanto, el sistema resiste el ataque de *brute-force*.

C. Ataque de shoulder-surfing

El ataque de mirar-sobre-el-hombro o *shoulder-surfing* es la técnica que utiliza un atacante para observar la contraseña cuando el usuario "cree que nadie lo observa". Es un ataque ampliamente utilizado en cajeros automáticos para conocer el NIP (Número de Identificación Personal) asociado a la tarjeta.

La prueba se realizó con cinco usuarios que crearon una contraseña y superaron el proceso de autenticación en dos ocasiones. Un atacante estuvo observando en todo momento el proceso de creación de la contraseña gráfica personal y durante el proceso de autenticación a cada usuario.

En la primera fase del sistema, las imágenes se mostraban en un Jframe amplio, casi del tamaño del monitor, facilitando la observación. Por lo tanto, la versión final presenta las imágenes en un tamaño menor, dificultando la observación. Por lo tanto, el sistema resiste al ataque de *shoulder-surfing.*

VI. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo, se propone un sistema de autenticación basado en imágenes personales que brinda al usuario el poder de decidir el número de imágenes, escoger las imágenes y definir la secuencia que dará origen a la contraseña gráfica personal. Las imágenes pueden ser capturadas en el momento utilizando una cámara web o pueden ser cargadas desde cualquier dispositivo de almacenamiento.

El proceso de autenticación consta de dos desafíos que se pueden presentarse de manera individual o conjunta, incrementando la dificultad para el atacante. Además, las medidas de seguridad tradicionales robustecen el sistema propuesto. En base al análisis de seguridad, se determina que el sistema resiste los ataques de *brute-force*, *keylogger*, y *shoulder-surfing*.

El sistema de autenticación presentado fue implementado para entorno web, demostrando su viabilidad para una integración en la banca electrónica.

El trabajo futuro se encuentra orientado a la usabilidad del sistema con una población con edades entre 12 a 25 años de edad debido a que ese grupo de usuarios serán los que posiblemente utilicen este tipo sistemas de autenticación.

AGRADECIMIENTOS

Se agradece al Mtro. Abraham López Nájera y al Dr. Francisco López Orozco por sus valiosos comentarios y apoyo otorgado durante el desarrollo del proyecto. También se agradece a los revisores anónimos que contribuyeron a mejorar la calidad del trabajo. Este trabajo fue apoyado parcialmente por el proyecto 167859 de SEP-CONACyT- Ciencia Básica.

REFERENCIAS

[1] Almuairfi S., P. Veeraraghavan y N. Chilamkurti, A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices, *Mathematical and Computer Modelling,* vol. 58, nº 1-2, p. 108–116, 2013.

[2] Anderson, J. y G. Bower, Recognition and Retrieval Processes in Free Recall, *Psychological Review*, vol. 79, nº 2, pp. 97-123, 1972.

[3] Bentley J. y C. Mallows, How much assurance does a pin provide?, 2nd International Workshop on Human Interactive Proofs, Springer-Verlag Berlin Heidelberg, 2005, pp. 111-126.

[4] Biddle R., S. Chiasson y P. Van Oorschot, Graphical passwords: Learning from the first twelve years, *Journal ACM Computing Surveys*, vol. 44, nº 4, 2012.

[5] Blonder G., Graphical Password. United States Patente 5,559,961, 24 Septiembre 1996.

[6] Dhamija R. y A. Perrig, Déjà Vu: a user study using images for authentication, 9th conference on USENIX Security Symposium, 2000.

[7] Dhamija R. y J. Tygar, The battle against phishing: Dynamic Security Skins, Symposium on Usable privacy and security, 2005.

[8] Florencio D. y C. Herley, A large-scale study of web password habits, 16th Int. Conf. World Wide Web, 2007.

[9] Haber R., How we remember what we see, *Scientific American*, vol. 222, nº 5, pp. 104-112, 1970.

[10] Herzberg A. y R. Margulies, My Authentication Album: Adaptive Images-Based Login Mechanism, IFIP Advances in Information and Communication Technology 376, Springer Verlag, 2012, pp. 315-326.

[11] Irakleous I., S. Furnell, P. Dowland y M. Papadaki, An experimental comparison of secret-based user authentication technologies, *Information Management & Computer Security*, vol. 10, nº 3, pp. 100-108, 2002.

[12] Jali M., S. Furnell y P. Dowland, Assessing image-based authentication techniques in a web-based environment, *Information Management & Computer Security*, vol. 18, nº 1, pp. 43-53, 2010.

[13] Jermyn I., A. Mayer, F. Monrose, M. Reiter y A. Rubing, The Design and Analysis of Graphical Passwords, 8th conference on USENIX Security Symposium, 1999.

[14] Kim H. y J. Huh, PIN selection policies: Are they really effective?, *Computers & Security*, vol. 31, nº 4, pp. 484-496, 2012.

[15] Liu X., H. Gao, L. Wang y X. Chang, An Enhanced Drawing Reproduction Graphical Password Strategy*, Journal of Computer Science and Technology*, vol. 26, nº 6, pp. 988-999, 2011.

[16] Luo J. y M. Yang, A mobile authentication system resists to shoulder-surfing attacks, *Multimedia Tools and Applications*, vol. 75, nº 22, p. 14075–14087, 2016.

[17] Passfaces Corporation, http://www.passfaces.com/enterprise/resources/resources_page.htm, 2005. [En línea]. [Último acceso: 1 9 2016].

[18] Standing L., J. Conezio y R. N. Haber, Perception and memory for pictures: Single-trial learning of 2500 visual stimuli, *Psychonomic Science*, vol. 19, nº 2, pp. 73-74, 1970.

[19] Sun H., Y. Chen y Y. Lin, oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks, *IEEE Transactions on Information Forensics and Security*, vol. 7, nº 2, pp. 651-663, 2012.

[20] Taekyoung K. y J. Hong, Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks, *IEEE Transactions on Information Forensics and Security*, vol. 10, nº 2, pp. 278-292, 2015.

[21] Takada T. y H. Koike, Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images, International Conference on Mobile Human-Computer Interaction, Springer-Verlag Berlin Heidelberg, 2003, pp. 347-351.

[22] Wiedenbeck S., J. Waters, J. Birget, A. Brodskiy y N. Memon, PassPoints: design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, vol. 63, nº 1-2, pp. 102-127, 2005.

[23] Xingjie Y., W. Zhan, L. Yingjiu, L. Liang, T. Z. Wen y S. Li, EvoPass: evolvable graphical password against shoulder-surfing attacks, *Computers & Security*, vol. 70, pp. 179-198, 2017.

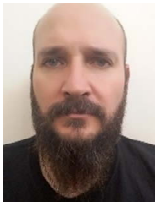
[24] Yan J., A. Blackwell, R. Anderson y A. Grant, The memorability and security of passwords - some empirical results, *IEEE Security & Privacy*, vol. 2, nº 5, pp. 25-31, 2004.

Pablo Abraham Sosa Valles es Ingeniero en Sistemas Computacionales por la Universidad Autónoma de Ciudad Juárez. Sus áreas de interés son seguridad informática, desarrollo web y base de datos. En estos momentos, se encuentra preparándose para ingresar a realizar sus estudios de postgrado en ciencias computacionales.

Javier Gerardo Villalobos Serrano es Ingeniero en Sistemas Computacionales por la Universidad Autónoma de Ciudad Juárez. Sus áreas de interés son seguridad informática, desarrollo web y base de datos. En estos momentos, se encuentra preparándose para ingresar a realizar sus estudios de postgrado en ciencias computacionales.

El Dr. Velarde actualmente se desempeña como profesor-investigador en el Área de Ciencias Básicas e Ingenierías de la Universidad Autónoma de Nayarit. Recibió el título de ingeniero en electrónica por la Universidad Autónoma de Guadalajara en 1993. Los grados de maestría y doctorado en ciencias por parte del Centro de Investigación y Estudios Avanzados del IPN (CINVESTAV-IPN) en 2001 y 2009, respectivamente. El Dr. Velarde es perfil PRODEP e investigador del Sistema Nacional de Investigadores (SNI). Sus principales líneas de investigación están relacionadas con el modelado del tráfico IP y el diseño de modelos estadísticos basados en entropía para sistemas de detección de intrusiones.

El Dr. Vicente García Jiménez es Ingeniero en Sistemas Computacionales, cursó su carrera en el Instituto Tecnológico de Villahermosa. Magíster en Ciencias en Ciencias Computacionales del Instituto Tecnológico de Toluca. En el 2010 obtiene el grado de doctor en sistemas informáticos avanzados en la Universitat Jaume I en Castellón de la Plana, España. Del 2010 al 2013 trabajó en diversos proyectos de aprendizaje automático y de visión por computadora en el Instituto de Nuevas Tecnologías de la Imagen en España. En el 2013, realizó un posdoctorado en el grupo de Procesamiento de Señales en la Universidad Autónoma de Ciudad Juárez. Ha publicado en revistas internacionales en diferentes áreas de la minería de datos. Actualmente es profesor titular B en la Universidad Autónoma de Ciudad Juárez. Sus temas de interés incluyen: minería de datos, procesamiento de datos, clasificación supervisada, problemas no balanceados, métricas de evaluación y valoración del riesgo crediticio, entre otros temas.



El Dr. Jorge Ramón Parra Michel es Ingeniero Electromecánico y actualmente es Profesor Investigador Titular de la Universidad De La Salle Bajío. Sus estudios Doctorales los realizó en el Centro de Investigaciones en Óptica. Ha sido distinguido como Miembro del sistema Nacional de Investigadores del CONACYT, es miembro del registro de evaluadores Iberoamericano, acreditados por RCEA en el área de Física, Matemáticas y ciencias de la tierra del CONACYT. También ha sido consultor científico para empresas del ramo energético y metalmecánico. El Dr. Parra se especializa en análisis de esfuerzos mecánicos mediante técnicas ópticas como la interferometría del patrón de Moteado, Correlación digital de imágenes y proyección de luz estructurada. Actualmente imparte cátedra en los programas de la maestría de Diseño de estructuras, Maestría en Ingeniería de sistemas mecatrónicos e Ingeniería Electromecánica de la Universidad de la Salle Bajío. Cuanta con varias publicaciones científicas y a su vez como miembro de comités editoriales de varias revistas de divulgación científica.

Luis J. Mena obtuvo una licenciatura en computación y una maestría en computación aplicada en la Universidad del Zulia, Venezuela. Posteriormente obtuvo el grado de doctor en ciencias computacionales en el Instituto Nacional de Astrofísica, Óptica y Electrónica, México. Actualmente es profesor-investigador de tiempo completo del programa académico de ingeniería en informática y líder del cuerpo académico consolidado "Tecnologías de la Información y Comunicaciones Aplicadas". Es Investigador Nacional del Sistema Nacional de Investigadores en el Área de Ingenierías e Investigador Honorifico del Sistema Sinaloense de Investigadores y Tecnólogos. Entre sus principales logros científicos destacan el desarrollo de nuevos algoritmos para medir la variabilidad de la presión arterial y para extraer patrones a partir de conjuntos de datos no balanceados. Además, ha publicado más de 40 artículos arbitrados en revistas indexadas y memorias de congresos nacionales e internacionales de prestigio, y sus intereses de investigación incluyen la minería de datos orientada al diagnóstico y pronóstico médico, y el desarrollo de aplicaciones móviles para el monitoreo personal de la salud.

Rafael Martínez Peláez es Doctor por la Universidad Politécnica de Cataluña e Ingeniero en Sistemas Computacionales por la Universidad del Valle de México en 2010 y 2003, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad de la Salle Bajío y miembro del Sistema Nacional de Investigadores (S.N.I.) con el nombramiento de Nivel 1. Es coautor de más de cuarenta artículos científicos publicados en revistas y congresos. Sus áreas de interés son autenticación, seguridad en servicios electrónicos, y privacidad en redes sociales.