OGMIOS: Verificación de Identidad y Recuperación de Cuentas en Mecanismos de Autenticación Sin Contraseñas

Miguel Barrera, Rubén Gaviria
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Diciembre 2019

1. Introducción

La autenticación es uno de los métodos fundamentales para la protección de un sistema, ayuda a reducir el riesgo de acceso no autorizado a la información, la infraestructura de comunicaciones y sus componentes. Al ser uno de los métodos más importantes de seguridad, lo hace principal objetivo a todo tipo de ataques, como el robo de credenciales y la pesca de contraseñas (phishing), que son vectores de ataque muy bien conocidos, pero que a pesar de los esfuerzos que se han realizado por parte de la academia y la industria, siguen siendo efectivos para obtener acceso a los sistemas de información protegidos por mecanismos de autenticación.

Los esquemas de autenticación que sirven para verificar la identidad de un usuario, como requisito para permitir el acceso a los recursos del sistema, se descomponen en tres:

1. *Factor basado en conocimiento*: Se fundamenta en lo que el usuario sabe, como usuarios y contraseñas de texto o contraseñas gráficas.
2. *Factor basado en la posesión:* Es lo que un usuario posee, depende de una posesión física, como tarjetas inteligentes, dispositivo (*token*) hardware con contraseña de un solo uso (OTP) o dispositivos móviles.
3. *Factor basado en la inherencia:* Consta en lo que el usuario es, como reconocimiento facial, biometría, huellas dactilares o reconocimiento de voz. [1]

En la tabla 1, se listan los principales problemas de cada factor de autenticación.

Tabla 1. Costos y desventajas de los esquemas de autenticación.

Esquema	Método de autenticación	Costo de implementación	Riegos
Basado en el conocimiento	-Usuario y contraseña - Código (PIN) - Patrón de bloqueo - Contraseña gráfica - Respuesta al desafío	Bajo (no requiere hardware adicional)	- Baja entropía - Difícil de recordar - Susceptible a ataques de diccionario - Permite el espionaje

			- Preguntas de seguridad publicas
Basado en la posesión	- Llave física -Tarjeta inteligente -Comunicación (NFC) -Hardware token - Celular	Medio (contempla dispositivos adicionales)	- Pérdida - Robo - Deterioro
Basado en la inherencia	- Huella dactilar - Palma de la mano - Iris - Voz - Rostro	Alto (dependiendo de la complejidad del dispositivo biométrico)	- Falsos negativos y Falsos positivos - No es posible cambiar ni recuperar el factor biométrico en caso de compromiso. - El factor no es secreto - El usuario tiene poco control si existe un error de autenticación

Nota: Adaptado de [2]-[4].

Es difícil encontrar un factor de autenticación que sea inmune a todas las amenazas posibles, pero una combinación de técnicas que complementen sus fortalezas para reducir sus debilidades ante diferentes ataques es lo recomendado [3].

Es por esto que el objetivo de este trabajo es evaluar diferentes factores de autenticación y seleccionar el que tenga menor nivel de riesgo, identificando en este sus principales problemas y proponer una manera de mitigarlos.

2. Propuesta

En la revisión del estado del arte, el factor por posesión representa un menor nivel de riesgo, con relación a los factores basado en conocimiento y el basado en la inherencia [3][4]. A pesar de esto, algunos retos aún siguen vigentes: el primero de ellos es la verificación de la identidad de la persona que se registra por primera vez en el sistema, y el segundo es la recuperación de cuentas de usuario cuando un autenticador por hardware ha sido robado, perdido o deteriorado por el uso.

La tabla 2 presenta una comparación con diferentes trabajos encontrados en el estado del arte. Como se puede apreciar, se ha utilizado principalmente técnicas de biometría para realizar la verificación de la identidad de los usuarios de un sistema.

Tabla 2 - Comparación de mecanismos de verificación de identidad

Factor de autenticación	¿Código abierto?	Tecnologías involucradas	Riesgos	Servicios o dispositivos
Biométrico con reconocimiento facial	No	Redes neuronales	Efectos de la edad, iluminación, fotografías públicas del usuario.	Cámaras fotográficas o de video embebidas en dispositivos de computo
Biométrico con reconocimiento de huellas	No	Comparación de patrones en la huella	Copia de la huella dactilar, suciedad del lector	Dispositivo lector de huellas
Biométrico con reconocimiento al caminar	No	Aprendizaje de máquina (Machine learning)	Nivel de aceptación y precisión.	Video cámaras con sensores de movimiento
Posesión	Sí	Contraseña de un solo uso	Perdida, robo, descuido del factor	Hardware
Biométrico con reconocimiento facial y voz	No	Aprendizaje de máquina (Machine learning)	Grabaciones de voz, fotografías	Cámaras fotográficas o de video y micrófonos embebidos en dispositivos de computo

Nota: Resumen [5]-[8]

La tabla 4 muestra algunos de los mecanismos más usados de recuperación, en el que se evidencia el problema de la verificación de identidad.

Tabla 3 - Comparación de mecanismos para recuperar la cuenta de usuario

Método	Vulnerabilidad	¿Verifica identidad?
Correo alternativo	Si el usuario tiene la misma clave para todas las cuentas.	No
Respuesta al desafío - Móvil	Hombre en el medio	No
Preguntas de seguridad	Las preguntas y respuestas son públicas, al conocer al usuario se pude responder correctamente	No
Conocimiento de la cuenta	La información de la cuenta puede ser accesible por cualquier persona	No

Nota: Resumen [9]-[11]

De tal manera que la propuesta consiste en diseñar un mecanismo de recuperación de cuentas de usuario, que garantice la autenticidad de este y la recuperación de su cuenta. Para esto el mecanismo que permite garantizar que el usuario es fidedigno, es el biométrico, por lo que la decisión es implementar el reconocimiento facial, ya que no requiere de un lector biométrico especializado [7].

Sin embargo, este método tiene grandes retos por su facilidad de vulnerar con elementos básicos, como situar una foto del usuario frente a la cámara y hacerse pasar por él.

Es por esto que adicionalmente se propone incorporar un factor de posesión, por si una persona que no es el usuario logra pasar el umbral de aceptación, deba presentar un factor de posesión para continuar.

En la ilustración 1, se detalla el diagrama de la arquitectura, con los componentes tanto hardware como software.

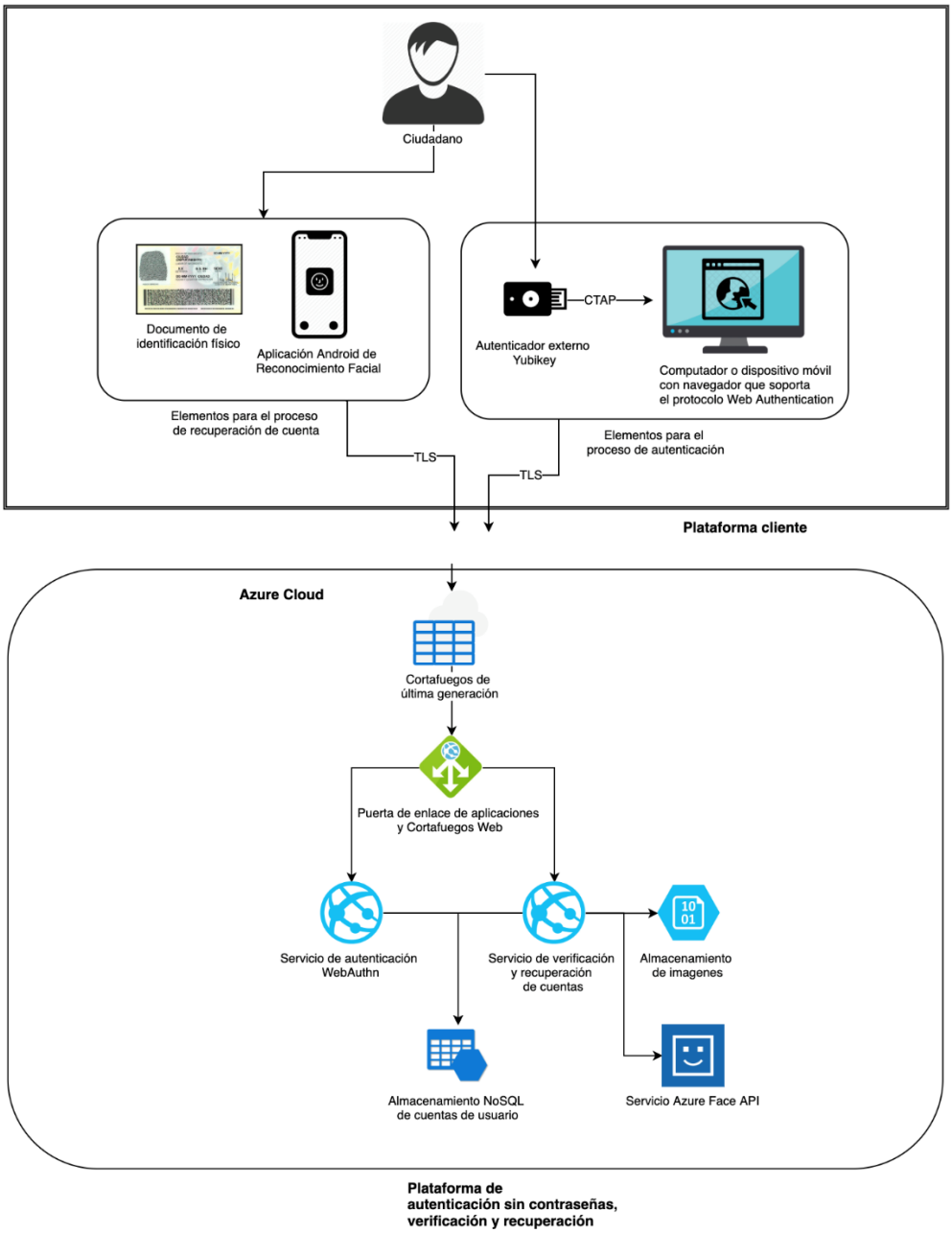

Ilustración 1- Arquitectura detallada de la solución

A continuación, se describen los componentes de la arquitectura de la solución:

Plataforma cliente

- Ciudadano: Representa al usuario de los servicios de identificación de identidad, autenticación y recuperación de cuenta de usuario.
- Documento de identidad físico: El cuál posee unas características particulares que permiten validar la identidad de cualquier ciudadano.
- Aplicación Android de reconocimiento facial: Aplicación móvil para el sistema operativo Android o de escritorio, que permite realizar reconocimiento facial de un ciudadano.
- Autenticador interno (Yubikey): Dispositivo hardware que permite generar material criptográfico para la autenticación de los usuarios del sistema, usando credenciales de llave pública y llave privada [3].
- Computador o dispositivo móvil: Para la comunicación con el servicio de autenticación en la nube.

Componentes del servicio

- Cortafuegos de última generación: Firewall que permite la inspección de paquetes en profundidad y es el encargado de la primera capa de protección a nivel de red en la infraestructura.
- Puerta de enlace: Permite el enrutamiento de las peticiones HTTP a los diferentes servicios del sistema.
- Almacenamiento: repositorio de cuenta de usuario basado en tecnologías NoSQL.
- Almacenamiento Blob: Repositorio de imágenes que permite almacenar la información biométrica de los usuarios, es usada tanto por el servicio Web de autenticación como el de recuperación de la cuenta.

Componentes de protección

- Servicio web de autenticación: Servicio web que permite registrar la identidad del usuario y la autenticación de este.
- Servicio de recuperación de la cuenta: Permite recuperar las cuentas de usuario a través del reconocimiento facial y la verificación de la información del documento de identidad del usuario.
- Servicio Face API: Servicio de Azure que implementa diferentes algoritmos de reconocimiento facial y que expone una API para ser integrado.

3. Evaluación

En la revisión del estado del arte no se encontraron estudios que permitan contar con métricas asociadas a los diferentes métodos de autenticación, para de esta manera comparar el esquema por contraseña, con el resultado de la solución propuesta. Como estrategia de validación, se adelantará un caso de estudio que permita verificar y comparar los criterios de seguridad, desempeño, costos, facilidad de implementación, escalabilidad y la experiencia de usuario; todo en un ambiente controlado bajo las mismas condiciones, y así poder comparar las métricas mencionadas anteriormente.

Por lo que, para evaluar la solución en un contexto real, desarrollamos un prototipo funcional, a fin de realizar pruebas de eficacia, eficiencia, de carga y facilidad de uso.

Tabla 4 - Resultados del estudio de caso.

Participante	Registro de Usuario	Autenticación de usuario	Verificación de identidad	Cierre de sesión	Recuperación de la cuenta
Participante 1	✓	✓	✓	✓	✓
Participante 2	✓	✓	✓	✓	x
Participante 3	✓	✓	✓	✓	✓
Participante 4	✓	✓	✓	✓	✓
Participante 5	✓	✓	✓	✓	✓
Participante 6	✓	✓	✓	✓	✓

La tabla 4 muestra las pruebas realizadas a seis participantes, donde para uno ellos, el proceso de la recuperación de la cuenta, le representó problemas por bloqueo de firewall en una red privada. Para los otros cinco participantes, todos los pasos fueron satisfactorios.

Así para medir la eficacia, se divide las pruebas satisfactorias, sobre el total de las pruebas. Por lo tanto, el resultado de la eficacia en las pruebas fue:

$$Ef = \frac{5}{6} * 100 = 83{,}33\%$$

Luego de verificar que el prototipo funciona, realizamos una encuesta a nueve empleados o estudiantes de la Universidad de los Andes, para medir la facilidad de uso de los pasos propuesto en la solución.

En la ilustración 2, se evidencian las preguntas y respuestas más relevantes de la encuesta, donde las primeras dos se centran en conocer la facilidad de uso de la solución, y las siguientes en la percepción del usuario.

Ilustración I1- Preguntas y respuestas más relevantes de la encuesta.

Cabe resaltar la facilidad que les representó a los usuarios el inicio de sesión, la apreciación de seguridad y el efecto de seguridad de la solución, respecto a un mecanismo tradicional que usa contraseñas.

Por último, luego de validar la eficacia y la facilidad de uso, se realiza el estudio de costos, para ver la viabilidad de crear una empresa, que venda proyectos con el desarrollo e implementación de la solución propuesta a empresas con alta transaccionalidad y manejo de información sensible. Dando como resultado un costo por transacción de $31 pesos Colombianos, producto de la operación en la nube con los servicios planteados en la arquitectura.

Todas estas transacciones presentan un reto a la seguridad de la información, pues según unas cifras señaladas por el periódico el tiempo, en el año 2015, los robos y fraudes bancarios a través de transacciones electrónicas pueden acercarse a $300.000 millones de pesos[1]. Adicionalmente Según la revista dinero: "El sector bancario registró 24 millones de transacciones electrónicas durante el primer semestre de 2017 y movilizó $64 billones"[2].

Con los indicadores mencionados, aunque no se encuentran para el mismo año, se realiza el cálculo de dinero perdido por transacción bancaria, donde las pérdidas para el año 2015 fueron $300.000 millones de pesos y el número de transacciones en el primer semestre del año 2017 fue de 24 millones, las perdidas por transacción son de $6.250 pesos. Cabe resaltar que estos estimados pueden ser más altos para el año 2019, ya que el número de transacciones incrementa cada año.

[1] Archivo del periódico el Tiempo: https://www.eltiempo.com/archivo/documento/CMS-16574145
[2] Reporte de la revista Dinero: https://www.dinero.com/empresas/articulo/transacciones-electronicas-en-colombia-en-2017/252058

Esto nos permite demostrar financieramente la viabilidad del proyecto, pues el costo de la transacción de la solución propuesta es mucho más bajo que las perdidas por transacción calculados con las cifras reportadas por el Tiempo y la revista Dinero.

Trabajo futuro

- Buscar alternativas o desarrollar un método de reconocimiento facial, que mida profundidad y otras características, que permitan identificar que el rostro que es capturado no esté siendo suplantado, con elementos como una fotografía o un video.
- Evaluar si el método de verificación de identidad de la solución propuesta en este trabajo es viable para verificar la identidad de la persona al momento de iniciar sesión; teniendo en cuenta las metodologías de usabilidad.

Conclusiones

- El uso de esquemas de autenticación basado en contraseñas puede ser reemplazado por soluciones basadas en posesión, uno de ellos es el Web Authentication, cuyo uso se está expandiendo en la industria al mejorar los niveles de seguridad mitigando los problemas bien conocidos como lo es el phishing, ataques de fuerza bruta, y robo de credenciales de acceso.
- El factor biométrico de reconocimiento facial y el factor por posesión con la cedula de ciudadanía colombiana es una solución viable para verificar la identidad y recuperar la cuenta de usuario que usa un factor de autenticación por posesión.
- Combinar dos o más métodos de autenticación ayuda a reducir las debilidades de cada esquema. En el proyecto, el factor por posesión ayuda a mitigar el problema de la precisión y el umbral de aceptación del reconocimiento facial; y este último, ayuda a demostrar que el propietario es quien tiene el factor por posesión.
- La usabilidad es un factor crítico a la hora de construir cualquier solución tecnológica, y en mayor medida, para sistemas que deben brindar capacidades para ser autogestionadas por los usuarios como lo es los procesos de registro, autenticación y recuperación de cuenta.

Referencias

[1] I. Velásquez, A. Caro, and A. Rodríguez, “Authentication schemes and methods: A systematic literature review,” *Information and Software Technology*, vol. 94. Elsevier B.V., pp. 30–37, 01-Feb-2018.
[2] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, “Authentication systems: A literature review and classification,” *Telematics and Informatics*, vol. 35, no. 5. Elsevier Ltd, pp. 1491–1511, 01-Aug-2018.
[3] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication,” in *Proceedings of the IEEE*, 2003, vol. 91, no. 12, pp. 2021–2040.
[4] K. Altinkemer and T. Wang, “Cost and benefit analysis of authentication systems,” *Decis.*

Support Syst., vol. 51, no. 3, pp. 394–404, Jun. 2011.
[5] D. B. Mei Yin, A.-A. Mukhlas, R. Z. Wan Chik, A. Talib Othman, and S. Omar, “A proposed approach for biometric-based authentication using of face and facial expression recognition,” in 3rd IEEE International Conference on Communication and Information Systems, ICCIS 2018, 2019, pp. 28–33.
[6]A. Makrushin and A. Wolf, “An overview of recent advances in assessing and mitigating the face morphing attack,” in 26th European Signal Processing Conference, EUSIPCO 2018, 2018, vol. 2018-Septe, pp. 1017–1021.
[7] A. Okumura, S. Komeiji, M. Sakaguchi, M. Tabuchi, and H. Hattori, “Identity Verification Using Face Recognition for Artificial-Intelligence Electronic Forms with Speech Interaction,” 1st International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019, held as part of the 21st International Conference on Human-Computer Interaction, HCI International 2019, vol. 11594 LNCS. Springer Verlag, NEC Solution Innovators, Ltd., Kawasaki, Japan, pp. 52–66, 2019.
[8] D. Valdes-Ramirez et al., “A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation,” IEEE Access, vol. 7, pp. 48484–48499, 2019.
[9] V. Jain, G. Chaudhary, N. Luthra, A. Rao, and S. Walia, “Dynamic handwritten signature and machine learning based identity verification for keyless cryptocurrency transactions,” J. Discret. Math. Sci. Cryptogr., vol. 22, no. 2, pp. 191–202, 2019.
[10] S. Lee and J. Kim, “A bifurcation-based descriptor for sclera recognition,” in 18th International Conference on Electronics, Information, and Communication, ICEIC 2019, 2019.
[11] A. Poosarala and R. Jayashree, “Uniform classifier for biometric ear and retina authentication using smartphone application,” in 2nd International Conference on Vision, Image and Signal Processing, ICVISP 2018, 2018.