ProTego

Autenticación Continua

Whitepaper

ProTego: DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND CARE CENTERS

Proyecto Nº 826284

Convocatoria: H2020-SU-TDS-02-2018. Trusted digital solutions and Cybersecurity in Health and Care

Resumen ejecutivo

Actualmente el modelo Zero-Trust rige los requisitos de seguridad en el ciberespacio. Este paradigma estipula que es imprescindible securizar cada uno de los dispositivos finales para mantener la seguridad del sistema. Para cumplir con este principio, entre otras cosas, hay que garantizar la integridad del control de accesos que permite acceder a un operario acceder al sistema. Se conoce como sistemas de autenticación continua a aquellos elementos que dentro de un sistema de control de accesos, sin requerir la participación activa del usuario, son capaces de determinar si su identidad sigue siendo la del usuario legítimo (el único que debería conocer las credenciales) o está siendo suplantado tras el proceso de autenticación. Con el objetivo de conocer tanto las tecnologías que pueden estar implicadas en las implementaciones de autenticación continua como los métodos de evaluación, y sus casos de uso, este whitepaper sintetiza el estado del arte de los sistemas de autenticación continua de una forma objetiva.

Este documento analiza los resultados científicos reportados presentando una imagen clara de: (1) qué fuentes de datos permiten la autenticación continua, (2) en qué sistemas se realiza, y (3) qué tratamiento se les puede dar para que esta autenticación sea lo más precisa posible; caracterizando al mismo tiempo qué dimensiones permiten conocer qué es y qué no es un sistema de autenticación continua.

Palabras clave

autenticación continua, biometría conductual, endpoint detection and response, zero trust

Introducción

El uso cada vez más intensivo de dispositivos portátiles con acceso a recursos críticos aumenta considerablemente la exposición de los activos de información a ser vulnerados. Un teléfono móvil o un ordenador portátil, que a efectos de arquitectura pueden actuar como puntos de entrada a toda la red de una organización, puede ser robado fácilmente, o incluso simplemente utilizado sin permiso del dueño en un despiste. Estos hechos ponen de manifiesto la necesidad de verificar constantemente la legitimidad del usuario para utilizar los recursos móviles.

Por otro lado, el modelo de amenazas clásico basado en la seguridad perimetral ya no es sostenible (*Cómo implementar un modelo Zero Trust de forma segura*, s. f.) si tenemos en cuenta tanto la distribución de los activos en la nube como la necesidad de flexibilización de las interconexiones entre sistemas. El nuevo paradigma de securización basado en el modelo Zero Trust (Computer Security Division, 2019) exige la creación de nuevas medidas para proteger el acceso a los recursos de cada sistema final.

Dentro del paraguas tecnológico conocido como Endpoint Detection and Response (EDR) (*Named*, 2013), se contemplan sistemas de respuesta ante atacantes mediante la detección de patrones de uso anómalos. El objetivo de este trabajo es determinar cómo defender los recursos cuando el ataque aprovecha un fallo en el sistema de autenticación, bajo la premisa de que existen patrones conductuales que no puede suplantar de ninguna manera. La herramienta que nos permitirá hacerlo es la autenticación continua.

¿Qué es la autenticación continua?

La autenticación continua se define, dentro de un sistema de control de accesos, como una fase tras la autenticación que permite validar si el usuario que se ha autenticado sigue siendo quien dice ser a lo largo de una sesión (BioCatch, s. f.), protegiendo los activos de información en el caso de que se produzca un acceso al sistema por parte de un atacante, o sus credenciales "clásicas" (i.e., el algo que tiene, sabe o es) hayan sido vulneradas.

Aunque cualquier interacción con un dispositivo deja huella (Mistek et al., 2019), no resulta fácil determinar cuántas interacciones realmente diferentes pueden existir, ni cuáles de ellas pueden ser lo suficientemente significativas como para atribuirlas a un usuario concreto (i.e., autenticarlo). Para lograr la autenticación continua tenemos que implementar mecanismos para que la máquina sea capaz de identificar a través de sus periféricos qué hay al otro lado.

Dividiremos los sistemas de autenticación continua en dos grandes familias, en función de las capacidades que tengan para sintetizar la identidad de la entidad evaluada:

1. **Sistemas de autenticación continua basados en sesión**

   La fiabilidad de estos sistemas estará determinada por la capacidad que tenga de determinar si la entidad ha cambiado o sigue siendo la misma durante toda la sesión, independientemente de la entidad que sea. Esto quiere decir, por ejemplo, que un sistema sería capaz de identificar si la persona que estaba utilizando la máquina al iniciar la sesión sigue siendo la misma durante toda ella. Deben tener una tasa de falsos negativos (FRR), o tasa de insulto, baja.

2. Sistemas de autenticación continua basados en huella conductual

Estos sistemas son los más ambiciosos, y los que más información pueden sintetizar de la entidad evaluada. La autenticación basada en huella es la que es capaz de generar una huella (como la huella dactilar) de la entidad, de forma que podría identificarla sin más información que la de su conducta. La fiabilidad de estos sistemas se determinará en base a la capacidad que tengan de diferenciar la entidad de forma unívoca frente a todas las demás. Su tasa de falsos positivos (FAR), o tasa de fraude, debe ser casi nula.

Por otro lado, en función de si los parámetros recogidos van a ser válidos a largo plazo o no, diferenciaremos entre:

1. Hard biometrics (entre sesiones)

Biometría (física o conductual) que no va a cambiar a lo largo del tiempo de vida del sistema, que va a cambiar muy ligeramente, o que se va a mantener mucho tiempo.

2. Soft biometrics (durante las sesiones)

Biometría efímera, que puede durar desde unas pocas semanas a, exclusivamente, una sola sesión (como puede ser el color de la ropa).

Para que además está autenticación continua sea viable desde el punto de vista de la usabilidad del sistema, no debe interrumpir el trabajo del usuario (o no constantemente, por ejemplo, pidiendo que realice una acción), si no que debe tener un perfil pasivo.

Al margen de que las aplicaciones más intuitivas de la autenticación continua son las que permiten desarrollar este proceso autenticando usuarios humanos, lo cierto es que todas estas técnicas son aplicables para autenticar otras entidades.

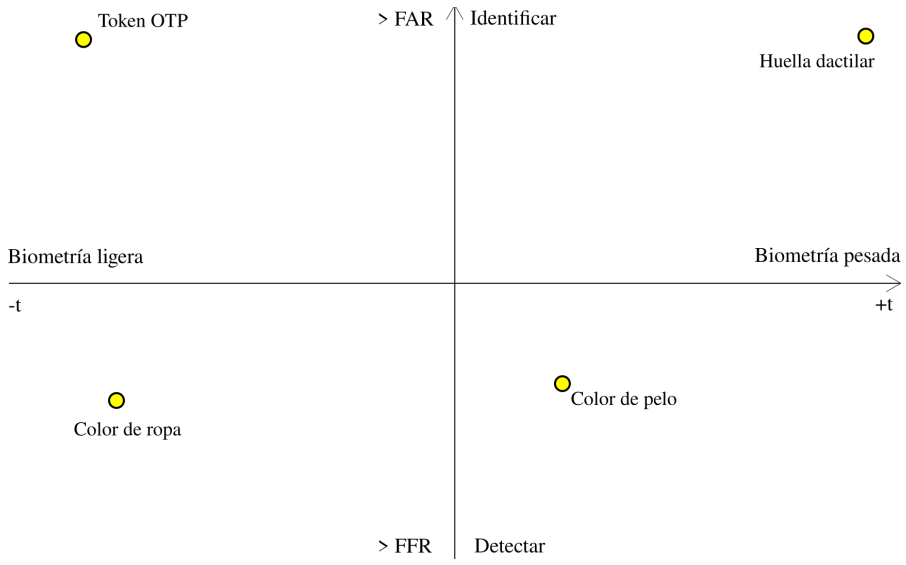

Figura 1 - Mapa permanencia/distintividad de autenticación continua

En este documento, fruto de un estudio sistemático de la literatura en el que se han analizado múltiples artículos artículos de diferentes fuentes con revisión por pares, mostraremos al lector qué tecnologías de autenticación continua existen, y qué métricas permiten evaluar su eficacia de una manera uniforme.

Biometría conductual

La biometría conductual es la caracterización de los patrones de comportamiento y de hábitos medibles. Por ejemplificar a través de actos cotidianos, no todas las personas se sientan de la misma forma en una silla, aliña en el mismo orden una ensalada (García-Chamizo & Nieto-Hidalgo, 2015), o incluso cambia de marchas igual en un vehículo. Y tampoco ejecutamos la misma acción de la misma forma en contextos distintos (e.g., no sujetamos el teléfono de la misma forma sentados que tumbados). La Figura 1 muestra algunos elementos biométricos que pueden servir de para identificar a un usuario, categorizados por su permanencia

Adquisición de parámetros biométricos

La mayor parte de las investigaciones se centran en la adquisición de parámetros biométricos de personas, pero algunas entidades no humanas (e.g., ordenadores, sensores, etc.) también siguen patrones conductuales únicos, como los mostrados en (Wang et al., 2019), donde se indica un método para autenticar máquinas mediante el análisis de la radiación electromagnética que producen. Aunque en estos casos no podamos hablar de biometría como tal (porque no hay *bio*), sí que podemos asimilarlo.

En la literatura analizada, la biometría conductual se obtiene eminentemente a través de teléfonos móviles (en un 40% de los casos), frente a un 13% de ordenadores. Sólo una investigación detecta patrones identificables mediante el mismo procedimiento en los dos tipos de sistema, y otra sirve para realizar autenticación continua a través de gafas inteligentes (Chauhan et al., 2016). Las restantes fuentes no indican que la autenticación se produzca frente a ningún dispositivo concreto, pero sí hablan de casos de uso como autenticar conductores que suben y bajan del vehículo (transportistas), o vigilar puestos de trabajo en una oficina (que podría asociarse principalmente a ordenadores de sobremesa).

Los principales periféricos utilizados para obtener datos del actor a autenticar son:

- **Pantalla táctil**

  Principalmente buscando captar gestos característicos de un usuario, pero también como sistema de precisar la forma de uso del teclado.

- **Sensores de teléfonos móviles**

  El acelerómetro, el giroscopio o el magnetoscopio del teléfono suelen usarse como complemento a otras mediciones, ayudando a contextualizar la actividad del usuario; aunque por sí solos también pueden servir para caracterizarlo(Sitová et al., 2016).

- **Cámara**

Principalmente mediante reconocimiento facial, y evaluación de datos de biometría ligera como ropa utilizada a lo largo de la sesión, color de pelo, uso de gafas, etc.

➔ **Teclado y ratón**

Los patrones de uso de ambos dispositivos, presentes en todos los ordenadores (también teclados virtuales en teléfonos móviles) también pueden servir para identificar, o completar la identificación de un usuario.

También son especialmente interesantes las investigaciones relacionadas con la medición de actividad cerebral (Nakanishi & Yoshikawa, 2015; Shozawa et al., 2013), pero su puesta en marcha es muy compleja (i.e., requieren hardware muy específico, e incluso condiciones de trabajo muy específicas). El resto de investigaciones (a excepción de (Eberz et al., 2016) que requiere una cámara especial) pueden aplicarse a sistemas bastante comunes, algunas incluso sólo accediendo a logs del sistema.

Procesamiento de datos

Una vez recogidos los datos se utilizan distintas técnicas de inteligencia artificial para generar modelos que permitan su evaluación de forma eficiente. Sin pretender nada más que ilustrar en qué casos de uso se aplica cada uno de ellos (sin entrar al detalle de cómo funcionan), podemos distinguir:

➔ **Support Vector Machine (SVM)**

Es la técnica de clasificación más utilizada. Consiste en la construcción de un hiperplano (lineal, polinómico o radial) que separe conjuntos de datos. En función del tipo de muestras que contenga nuestro dataset, se utilizará:

◆ **SVM “puro”**

Cuando se tienen al menos dos conjuntos de datos, se puede aplicar SVM para diferenciar los valores generados por el actor genuino del resto de valores posibles generables por otros actores. De esta forma, si tuviésemos datos de 100 usuarios, podríamos generar un modelo que nos permitiese diferenciar a uno de ellos de los 99 restantes.

◆ **One-class SVM**

SVM cuando sólo se tiene un dataset. Es decir, sólo tenemos datos del usuario legítimo y queremos diferenciarlo de todo lo demás.

➔ **k-nearest neighbors**

Otro procedimiento de agrupación es el método de los k-vecinos más cercanos, consistente en evaluar la densidad de los diferentes subconjuntos de datos contenidos el dataset para crear agrupaciones, y de esta forma saber cuándo un dato pertenece o no a un grupo.

➔ **Eigenfaces**

Es un método de reconocimiento facial basado en la reducción de las imágenes faciales a una serie de vectores característicos, generando una base facial (ver Figura 2 - Ejemplo de

modelos de eigenfaces (Wikimedia Commons,...) *F*, y almacenando la identidad de cada usuario como la variación que habría que introducir en *F* para obtener de nuevo su cara.

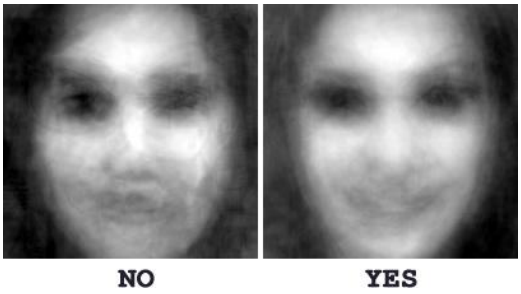

Figura 2 - Ejemplo de modelos de eigenfaces (Wikimedia Commons, 2019)

➔ **Interactive Artificial Bee Colony (IABC)**

En la investigación (Tsai et al., 2014), utilizan IABC como mecanismo de optimización del método de las *eigenfaces*. Imitando el comportamiento de los distintos participantes de una colmena en la búsqueda de recursos, este algoritmo da soporte a la toma de decisiones.

➔ **Red neuronal artificial**

Enlazando los resultados de un conjunto de sistemas de toma de decisiones, de una forma similar a la conexión existente entre las neuronas reales, permite imitar los mecanismos que utiliza el cerebro para reconocer patrones (de Lima e Silva Filho & Roisenberg, 2006; Popovici et al., 2014).

➔ **State-Space Models**

Cuando la forma más evidente de plantear el problema es codificarlo como un diagrama de estados (como es el caso de(Mahbub et al., 2018)), pueden utilizarse métodos simples, como los árboles de decisión, *Random Forests* en (Smith-Creasey & Rajarajan, 2019) (similar a una colección de árboles de decisión); o modelos de decisión basados en procesos de Markov, como Cadenas de Markov o Modelos Ocultos de Markov (Popovici et al., 2014; Roy et al., 2014).

➔ **Otros modelos probabilísticos**

En (Smith-Creasey & Rajarajan, 2019) comparan los resultados de utilizar distintos modelos, como regresión logística, o clasificadores bayesianos (i.e., *Naive Bayes*). En (Ananya & Singh, 2018) y (Acar et al., 2018) usan modelos estadísticos básicos (como media y desviación típica)

Autenticación continua

Una vez procesados los datos de biometría conductual (la Figura 3 muestra una relación de cómo los datos extraídos a través del estudio de la biometría conductual, pueden ayudar a autenticar de forma continua a una entidad), se debe establecer un mecanismo que permita, en función de las necesidades del sistema a proteger, detectar las acciones a tomar por el sistema de control de acceso. En función de cuánto se asemejan los datos de biometría conductual, al modelo existente, se determinará un nivel de confianza en la identidad del usuario; pero para ello hay que conocer la fiabilidad de dicho modelo.

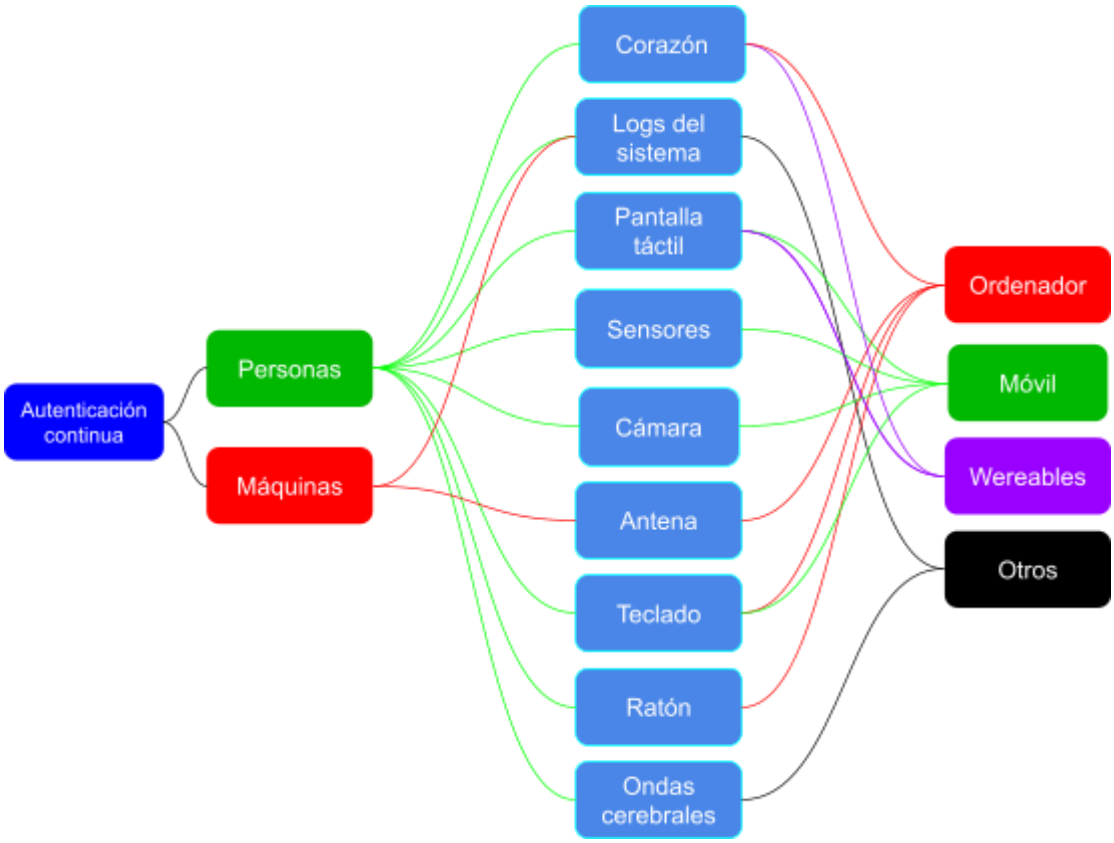

Figura 3 - Relación de componentes de autenticación continua

Métricas empleadas en la evaluación de resultados

Al tratarse a fin de cuentas de sistemas de autenticación, los términos utilizados para evaluar su eficacia son similares a las métricas utilizadas para calificar los algoritmo de entrenamiento. Los resultados son evaluados en los siguientes términos:

➔ **False Acceptance Rate**

Tasa para determinar la cantidad de veces que un impostor se haría pasar exitosamente por un usuario legítimo.

➔ **False Rejection Rate**

También conocido como tasa de insulto, es un índice de los usuarios genuinos que el sistema no ha sido capaz de reconocer y han sido bloqueados.

➔ **Equal Error Rate**

Es el valor en el que ambas tasas se igualan. Sirve para medir la eficacia del sistema de una forma más global. Si esta tasa es superior al 50% (valor en el que equivale a realizar la evaluación de forma aleatoria) el sistema es completamente arbitrario.

Ninguno de los sistemas evaluados en la literatura existente muestra cifras totales de EER superiores al 30%, y si bien alguno afirma llegar a tener una eficacia de prácticamente el 100%, sólo consiguen estas cifras en casos de uso y bajo unas condiciones de experimentación muy concretas.

Tipos de autenticación

En la Figura 4 - Tipo de sistema CA (1: CA de... puede verse que aunque la mayor parte de los sistemas existentes consiguen aproximaciones que dan una imagen fiable del usuario, y duradera en el tiempo, ninguno consigue crear una huella única del actor que evalúa. La ausencia de sistemas basados puramente en autenticación continua de sesión puede deberse a que un sistema de este tipo por sí solo, aporta poco valor a la seguridad de los activos, pero puede dar un plus de eficacia a otras aproximaciones (como la utilización de biometría ligera en (Tsai et al., 2014)).

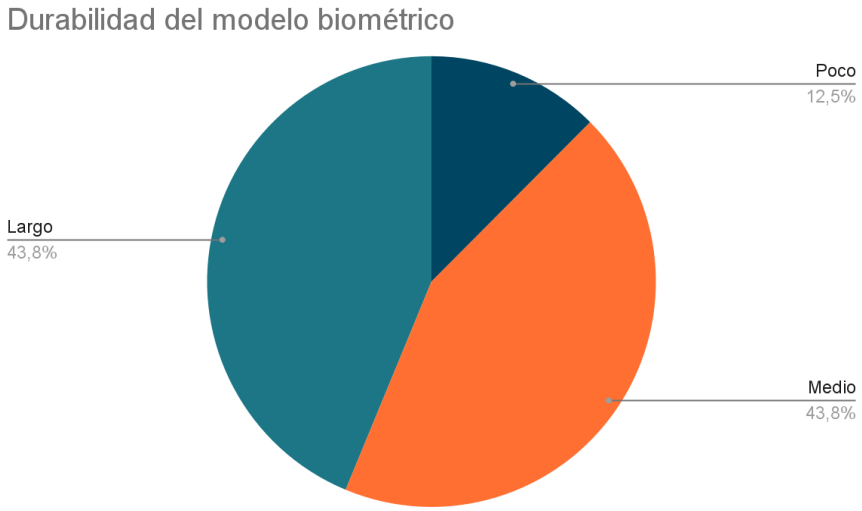

Figura 4 - Tipo de sistema CA (1: CA de sesión, 5: CA de huella conductual)

Esto apoya también el modelo de caracterización del usuario en las dimensiones *permanencia/distintividad* presentado inicialmente en este documento (Figura 1). No obstante existen

taxonomías adicionales como del estudio de Bamasag & Youcef-Toumi (2015), que divide los mecanismos de autenticación continua en base a cuatro dimensiones:

- **Universalidad**

  Puede ser utilizado con cualquier actor cubierto por el alcance del mecanismo (es decir, si identifica personas, sirve para identificar a cualquier tipo de persona).

- **Distintividad**

  Cuánto permite diferenciar al individuo de la población (i.e., si puede decir si el actor evaluado es X o es Y, o sólo tiene la capacidad de determinar “eras X, y ya no lo eres”.

- **Permanencia**

  Durante cuánto tiempo es válido el modelo generado sin reentrenarlo. Es decir, cuánto tiempo permanece inalterado el comportamiento del actor (lo que llamamos de huella).

- **Recolectabilidad**

  La característica o características que permiten la autenticación continua pueden ser codificados (debe ser, de alguna forma, medible cuantitativamente).

En la investigación de Smith-Creasey & Rajarajan (2019) también añaden:

- **Eficiencia**

  Para sistemas en teléfonos móviles, que son dispositivos con pocos recursos, y cuya autonomía depende del consumo de batería.

- **Aceptabilidad**

  Determina el grado de invasión que la solución supone para el entorno del usuario.

- **Tasa de burla**

  A diferencia de las tasas de error, la tasa de burla evalúa las garantías que ofrece el sistema para evitar que un atacante pueda recrear la identidad del sujeto legítimo.

Autenticación continua aplicada

Autenticación continua en ordenadores

La autenticación continua no sólo incrementa la seguridad del sistema, sino que además busca mejorar la seguridad de una forma poco invasiva. Uno de los principios de la autenticación continua es aumentar la usabilidad de los sistemas. Frente a pedir continuamente o cada cierto tiempo, datos de autenticación a un usuario, un sistema de autenticación continua puede trabajar de forma transparente al usuario. Interactuando solamente con el usuario en el caso de que haya problemas.

Aplicado a entornos de escritorio y web puede servir tanto como una medida que garantiza la presencia del usuario (frente a los clásicos salvapantallas que se activan tras cierto tiempo de inactividad), o como segundo factor de autenticación.

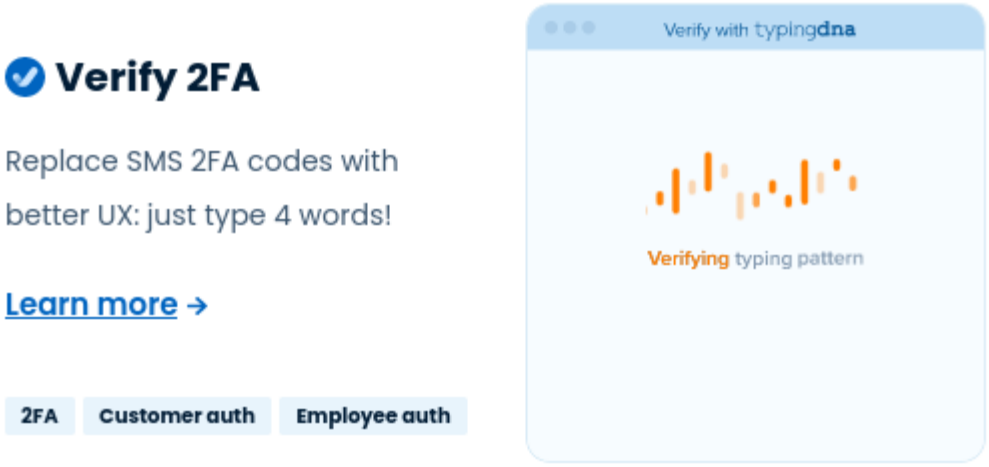

Figura 5. Ejemplo de verificación de identidad en TypingDNA

Esta última aproximación es una de las funcionalidades que ofrecen sistemas como TypingDNA[1] (ver Figura 5), que tras caracterizar la forma de escribir del usuario, permite integrarlo en el sistema de control de accesos de cualquier servicio web.

Autenticación continua en teléfonos móviles

Los teléfonos móviles son activos de información extremadamente valiosos, pero debido a sus características (i.e., tamaño, deslocalización, etc.) están expuestos a robos y extravíos que pueden comprometer la confidencialidad del usuario.

[1] TypingDNA: New Verify 2FA solution alternative to SMS OTP. https://www.typingdna.com/

Aunque hay ciertos patrones de uso que pueden ser similares a los de los ordenadores, estos dispositivos presentan particularidades, y además cuentan con numerosos periféricos (e.g., cámara, acelerómetro, etc.) que pueden enriquecer el proceso de caracterización de la biometría conductual.

Dos de los estudios más relevantes son HMOG y Touchalytics. Entre los dos cubren tanto la caracterización de los gestos realizados por el usuario en la pantalla (e.g., a la hora de escribir, o de desplazarse a través de las aplicaciones), como la influencia que tienen la forma de coger el dispositivo o la actividad que está realizando el usuario en paralelo a la hora de evaluar estos parámetros.

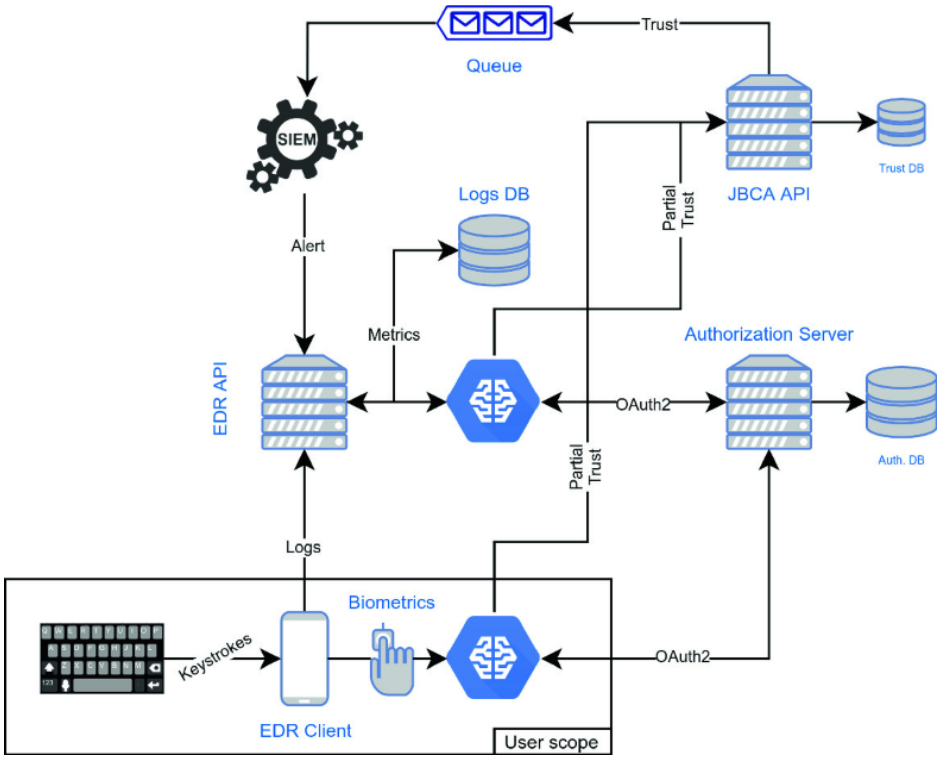

Figura 6. Arquitectura del subsistema de autenticación continua del proyecto ProTego (Junquera-Sánchez et al., 2021)

La aplicación de la autenticación continua en entornos móviles puede permitir el uso de cada vez más sistemas de información cuya seguridad es crítica, como sistemas médicos que manejen datos sensibles, o que aseguren la integridad de los datos de salud introducidos en el dispositivo. Una de las vías de investigación desarrolladas en el proyecto ProTego[2] se centra en garantizar la identidad de los usuarios presentes en entornos sanitarios a través de diferentes aproximaciones basadas en autenticación continua (ver Figura 6).

[2] BYOD and health sector. https://protego-project.eu/2020/06/byod-and-health-sector/

Conclusiones

La autenticación continua permite comprobar la identidad del usuario en cualquier momento. Es un mecanismo complementario para incrementar la seguridad en algunos entornos, como las aplicaciones móviles o IoT, o en determinados contextos, como los que manejan datos sensibles. Los sistemas de autenticación continua se pueden dividir en sistemas basados en sesión y sistemas basados en huella digital (o conductual). Para construir la huella digital se puede capturar y analizar la interacción del usuario, por ejemplo su uso del teclado en un ordenador, o de la pantalla táctil y los datos de los sensores de los teléfonos móviles. Estos datos se procesan mediante inteligencia artificial o aprendizaje máquina (machine learning) para construir modelos que representan la interacción del usuario y ante los que se pueden evaluar nuevas interacciones para determinar si pertenecen a la misma persona o es otra persona la que está usando el dispositivo. La permanencia en el tiempo de los modelos de usuario y su capacidad para distinguir entre usuarios son las principales características del sistema final. Los sistemas de autenticación continua se evalúan por su tasa de aceptación de usuarios legítimos y por su tasa de rechazo de accesos ilegítimos. En la práctica existen soluciones comerciales de autenticación continua basada en patrones de escritura (typping patterns) para ordenadores tradicionales. Los sistemas de autenticación continua para dispositivos móviles están siendo investigados en múltiples contextos, como en el proyecto ProTego.

Las investigaciones existentes demuestran el impacto de la autenticación continua en la protección, pero ponen de manifiesto que todavía queda un largo camino por recorrer hasta generar una huella única y duradera que permita la autenticación no invasiva del usuario. Este aspecto de la generación de una huella digital, que sea fácil de obtener discretamente y de la que el usuario no puede desprenderse, también nos plantea la necesidad de desarrollar un estudio ético formal, y de impacto para la privacidad de los datos personales. Por otro lado, la aplicabilidad de estos sistemas de análisis de identidades a otros actores no humanos (como la autenticación entre máquinas mostrada en (Wang et al., 2019)) abre la puerta a su uso para securizar entornos industriales o relacionados con el IoT.

Agradecimientos

Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea (proyecto No. 826284)

Referencias

Acar, A., Aksu, H., Uluagac, A. S., & Akkaya, K. (2018). WACA: Wearable-Assisted Continuous Authentication. *arXiv:1802.10417 [cs]*. http://arxiv.org/abs/1802.10417

Ananya, & Singh, S. (2018). Keystroke Dynamics for Continuous Authentication. *2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, 205-208. https://doi.org/10.1109/CONFLUENCE.2018.8442703

Bamasag, O. O., & Youcef-Toumi, K. (2015). Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme. *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, 1-8. https://doi.org/10.1145/2818362.2818363

BioCatch. (s. f.). *From Login to Logout: Continuous Authentication with Behavioral Biometrics*. Recuperado 4 de julio de 2019, de https://www.biocatch.com/resources/white-paper/from-login-to-logout-continuous-authentication-with-behavioral-biometrics

Chauhan, J., Asghar, H. J., Mahanti, A., & Kaafar, M. A. (2016). Gesture-Based Continuous Authentication for Wearable Devices: The Smart Glasses Use Case. En M. Manulis, A.-R. Sadeghi, & S. Schneider (Eds.), *Applied Cryptography and Network Security* (pp. 648-665). Springer International Publishing. https://doi.org/10.1007/978-3-319-39555-5_35

Cómo implementar un modelo Zero Trust de forma segura. (s. f.). Recuperado 3 de diciembre de 2019, de https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/8772-como-implementar-un-modelo-zero-trust-de-forma-segura.html

Computer Security Division, I. T. L. (2019, septiembre 23). *Zero Trust Architecture: Comment on Draft NIST SP 800-207 | CSRC*. CSRC | NIST. https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207

de Lima e Silva Filho, S. R., & Roisenberg, M. (2006). Continuous Authentication by Keystroke Dynamics Using Committee Machines. En S. Mehrotra, D. D. Zeng, H. Chen, B. Thuraisingham, & F.-Y. Wang (Eds.),

Intelligence and Security Informatics (pp. 686-687). Springer. https://doi.org/10.1007/11760146_90

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2016). Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics. *ACM Transactions on Privacy and Security*, *19*(1), 1:1-1:31. https://doi.org/10.1145/2904018

García-Chamizo, J. M., & Nieto-Hidalgo, M. (2015). Formalización algebraica del método de arriba hacia abajo de diseño tecnológico. *Undefined*. https://www.semanticscholar.org/paper/Formalizaci%C3%B3n-algebraica-del-m%C3%A9todo-de-arriba-hacia-Garc%C3%ADa-Chamizo-Nieto-Hidalgo/515c8e779c2b4a209670b0421de35644a023dd8e

Junquera-Sánchez, J., Cilleruelo-Rodríguez, C., de-Marcos, L., & Martínez-Herráiz, J. J. (2021). JBCA: Designing an Adaptative Continuous Authentication Architecture. En L. M. Bergasa, M. Ocaña, R. Barea, E. López-Guillén, & P. Revenga (Eds.), *Advances in Physical Agents II* (pp. 194-209). Springer International Publishing. https://doi.org/10.1007/978-3-030-62579-5_14

Mahbub, U., Komulainen, J., Ferreira, D., & Chellappa, R. (2018). Continuous Authentication of Smartphones Based on Application Usage. *ArXiv:1808.03319 [Cs, Stat]*. http://arxiv.org/abs/1808.03319

Mistek, E., Fikiet, M. A., Khandasammy, S. R., & Lednev, I. K. (2019). Toward Locard's Exchange Principle: Recent Developments in Forensic Trace Evidence Analysis. *Analytical Chemistry*, *91*(1), 637-654. https://doi.org/10.1021/acs.analchem.8b04704

Nakanishi, I., & Yoshikawa, T. (2015). Brain waves as unconscious biometrics towards continuous authentication—The effects of introducing PCA into feature extraction. *2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 422-425. https://doi.org/10.1109/ISPACS.2015.7432808

Named: Endpoint Threat Detection & Response. (2013, julio 26). Anton Chuvakin. https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/

Popovici, E. C., Stancu, L. A., Guta, O. G., Arseni, S. C., & Fratu, O. (2014). Combined use of pattern recognition algorithms for keystroke-based continuous authentication system. *2014 10th International Conference on Communications (COMM)*, 1-4. https://doi.org/10.1109/ICComm.2014.6866686

Roy, A., Halevi, T., & Memon, N. (2014). An HMM-based behavior modeling approach for continuous mobile authentication. *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 3789-3793. https://doi.org/10.1109/ICASSP.2014.6854310

Shozawa, M., Yokote, R., Hidano, S., Wu, C.-H., & Matsuyama, Y. (2013). Brain Signal Based Continuous Authentication: Functional NIRS Approach. En I. Rojas, G. Joya, & J. Cabestany (Eds.), *Advances in Computational Intelligence* (pp. 171-180). Springer. https://doi.org/10.1007/978-3-642-38682-4_20

Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Transactions on Information Forensics and Security*, *11*(5), 877-892. https://doi.org/10.1109/TIFS.2015.2506542

Smith-Creasey, M., & Rajarajan, M. (2019). A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Computers & Security*, *83*, 140-150. https://doi.org/10.1016/j.cose.2019.02.001

Tsai, P., Khan, M. K., Pan, J., & Liao, B. (2014). Interactive Artificial Bee Colony Supported Passive Continuous Authentication System. *IEEE Systems Journal*, *8*(2), 395-405. https://doi.org/10.1109/JSYST.2012.2208153

Wang, J., Ni, M., Wu, F., Liu, S., Qin, J., & Zhu, R. (2019). Electromagnetic radiation based continuous authentication in edge computing enabled internet of things. *Journal of Systems Architecture*, *96*, 53-61. https://doi.org/10.1016/j.sysarc.2018.12.003

Wikimedia Commons. (2019, marzo 11). *Tinderbox eigenfaces models*. Wikipedia. https://en.wikipedia.org/w/index.php?title=File:Tinderbox_eigenfaces_models.jpg&oldid=887229639