Universidad de Alcalá

Programa de Doctorado D442: INGENIERÍA DE LA INFORMACIÓN Y DEL CONOCIMIENTO, Inteligencia Artificial aplicada

Defensa en profundidad en sistemas de control de accesos mediante autenticación continua

Tesis Doctoral presentada por

Javier Junquera Sánchez

2022

Universidad de Alcalá

Programa de Doctorado D442: INGENIERÍA DE LA INFORMACIÓN Y DEL CONOCIMIENTO, Inteligencia Artificial aplicada

Defensa en profundidad en sistemas de control de accesos mediante autenticación continua

Tesis Doctoral presentada por

Javier Junquera Sánchez

Directores

Dr. José Javier Martínez Herráiz

Dr. Luis de Marcos Ortega

Alcalá de Henares, 1 de diciembre de 2022

Agradecimientos

Por común que sea el agradecimiento a los directores, este no puede estar más lejos del puro protocolo. Al Prof. José Javier Martínez Herráiz, no sabría agradecerle lo suficiente todos estos años de apoyo, de confianza, y el empeño que ha puesto, frente a toda adversidad, porque hoy estemos donde estamos. Por profesor, no deja de ser maestro; y mentor de tantos, que resulta tremendamente injusto que, los que tenemos la oportunidad de escribir estas líneas, no sepamos hacerlo con la rotundidad que merece. Ha sido también un privilegio contar con el apoyo del Prof. Luis de Marcos, con quien, entre otras cosas, he aprendido a escribir; pero además, a leer: ahora estudio cada *paper*, cada TFG, y cada TFM que me pasa por delante, con la mirada improntada por sus consejos. Ojalá poder hacerle honor a este privilegio, y poder transmitir, al menos, una pequeña parte de lo que he recibido.

A Carlos Cilleruelo, porque este trabajo es tan mío como suyo: nos queda todavía mucho que guerrear. En cada página hay un pedacito de toda la gente que me ha acompañado en las diferentes cátedras de ciberseguridad. A riesgo de dejarme a alguien, gracias David, Schuller, Juan, Nico, Enrique, Kevin, Alex, Omaima, Jorge, Germán, Juan, Jesús, Natalia, y Eloy. Por descontado, a los amigos de Vetusta: Iván, Samira, y Julio.

Eternamente agradecido a la educación pública, y a haber tenido la suerte de caer en Alcalá. Cada vez tengo más claro, también, que, con los recursos abiertos que tenemos a nuestro alcance, lo de llamarnos autodidactas sería un poco tramposo; así que, de nuevo [1], ¡gracias Wikipedia!

A mis familias: biológica, política, y demás agregados. Y termino con un gracias, compañera.

Ítaca t'ha donat el bell viatge
Sense ella no hauries sortit

Constantino Cavafis / Lluís Llach

Resumen

La seguridad de los sistemas de información depende, en gran medida, de que el proceso de control de accesos funcione correctamente. Pero, en los modelos clásicos, la identidad del operador sólo se autentica en momentos puntuales. Tras décadas de implantación de dispositivos móviles en la sociedad [2], se encuentran presentes en prácticamente todos los procesos de negocio, pero estos activos sufren de debilidades en la gestión de su seguridad: no se ubican en perímetros de red bien definidos y bastionables, son más susceptibles de ser robados, etc.; y en un modelo clásico de control de accesos, una vez iniciada la sesión, careceríamos de medidas para combatir estas amenazas. Activar el proceso de autenticación periódicamente sería molesto y contraproducente, pero mediante biometría conductual (i.e., caracterizando la identidad de un usuario por cómo se comporta con el sistema), sí podría implementarse un sistema que validase la identidad del operador sin interferir en su sesión de trabajo: un sistema de autenticación continua. En esta tesis se aborda cómo la autenticación continua puede ayudar a mitigar los riesgos comentados, convirtiéndose en una tecnología diferenciadora al implantar medidas de defensa en profundidad en los sistemas de control de accesos.

Al no existir un criterio claro para definir la autenticación continua, en primer lugar se ha desarrollado un estudio sistemático de la literatura, que permite caracterizar este área de investigación. En el segundo artículo se plantea un caso de uso, donde se refuerza la seguridad de un sistema distribuido aplicando principios de la autenticación continua; evidenciando al mismo tiempo las carencias de los sistemas dinámicos, y acotando la definición de autenticación continua. Finalmente, se estudia, experimentalmente, el rendimiento de 7 algoritmos supervisados de clasificación en el ámbito de la autenticación continua. Este estudio, junto con los resultados previos, sirve de soporte a la toma de decisiones en la implantación de la autenticación continua. Fija una base homogénea de conocimiento, que permite comparar las particularidades de estos algoritmos en el procesado de datos de biometría conductual, y discute su utilidad en función de los requisitos del sistema de control de accesos.

Esta tesis evidencia que el uso de autenticación continua contribuye a la defensa en profundidad de los sistemas de control de accesos, especialmente, aunque exclusivamente, a la de aquellos con un operador cuya sesión de trabajo debe ser autenticada.

Palabras clave: autenticación continua, defensa en profundidad, biometría conductual, ciberseguridad.

Abstract

The security of information systems is highly dependent on the access control process, but this process's reliability lies, mainly, on the punctual authentication of the operator's identity. After decades of implantation, [2], mobile phone technologies are present in practically all the current business processes, but, regarding information security, they have several weaknesses: they do not always operate in trusted environments, are easier to steal, etc.; what, from the point of view of access control, derives in a total absence of mechanisms to protect the information system once the operator's identity has been authenticated. Asking for authentication periodically could be obtrusive for a working session, but by using behavioural biometrics, it could be possible to evaluate the operators' identity without disturbing them: this is continuous authentication. This PhD Thesis addresses, through three research articles, how continuous authentication could mitigate the new risks of the information systems, leading to a successful defence-in-depth model for access control systems.

While there is no one formal definition of what continuous authentication is, the first step has been developing a systematic literature review, which has led to characterize this research area. The second article describes a use case where continuous authentication principles reinforce the security of a distributed information system, making evident the differences between dynamic authentication systems and continuous authentication ones. Finally, we have conducted an experiment where 7 supervised classification algorithms have been tested, analyzing how, and with which particularities, they can lead to continuous authentication. This final research aims to give support to the decision-making processes where continuous authentication is needed, but also to fix a solid knowledge base that allows the comparison of these algorithms in regards the behavioural biometrics.

This PhD thesis evidences that continuous authentication contributes to the defence-in-depth of access control systems, especially for those where a human operator must be authenticated during a working session.

Keywords: continuous authentication, defence-in-depth, behavioural biometrics, cybersecurity.

Índice general

Índice de tablas

Glosario de términos

AAA	Sistemas de control de accesos que utilizan autenticación, autorización, y registros de auditoría (en inglés, se usa *accountability*).
aceptabilidad	Característica de un sistema de CA para ser aceptado por el operador, muy ligada a la usabilidad.
colectibilidad	Grado de facilidad para recabar un parámetro, del operador, que pueda ser utilizado en un sistema de CA.
EDR	Sistemas de protección de equipos terminales, basado en la detección de anomalías, y con capacidad de respuesta (del inglés, *Endpoint Detection and Response*).
eficiencia	Capacidad de un sistema de CA para trabajar sin restar recursos a otros procesos del sistema de información.
permanencia	Capacidad de un sistema de CA para identificar una entidad a lo largo de varias sesiones de trabajo espaciadas en el tiempo.
resistencia a burla	Capacidad de un sistema de CA para resistir a suplantaciones intencionadas.
servidor	Equipo informático, ubicado, normalmente en entornos internos de una organización, que ofrece recursos a diferentes clientes remotos.
singularidad	Capacidad de un sistema de CA para identificar unívocamente a una entidad.
terminal	Equipo cliente sobre el que trabajan los operadores del sistema de información.
TOTP	Código pseudoaleatorio que utiliza como semilla un secreto precompartido, y como elemento común, para la autenticación, el segmento de tiempo en el que se genera. Definido en el documento RFC 6238.
universalidad	Capacidad de un modelo de CA para ser utilizado en cualquier operador, independientemente de sus peculiaridades (e.g., un

Capítulo 1

Introducción

1.1 Introducción

El control de accesos es una pieza clave en el ámbito de la seguridad de la información [3]. En cualquiera de sus dimensiones (i.e., confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad) subyace la necesidad de determinar quién puede hacer qué sobre cuál recurso [4], así como de que todo quede registrado para ser auditado; del mismo modo que no es posible garantizar este control de acceso sin la criptografía, los mecanismos de segmentación de redes o la ejecución segura del software.

Tras la aparición del modelo *zero trust* [5] nos encontramos ante un escenario en el que: 1. los dispositivos ya no se encuentran protegidos por perímetros, y, 2. hay que garantizar la seguridad en cada uno de ellos sin poder depender de terceros. Para ello, el criterio más común es el del riesgo, de cara a evaluar con objetividad las medidas de seguridad que deben ser implementadas.

La gestión del riesgo parte de la identificación de los elementos que sustentan los procesos de negocio (i.e., activos) determinando qué amenazas pueden degradarlos, y con qué probabilidad. Se establecerán en consonancia medidas de seguridad que ayuden a protegerlos, y a detectar rápidamente si sufren dicha degradación para responder a la amenaza, y recuperar lo antes posible un estado seguro.

Heredado de la seguridad física, el concepto de defensa en profundidad [6] también es de aplicación en otros ámbitos [7], como es el caso de los sistemas de información. Este enfoque promueve la aplicación de diferentes medidas de seguridad independientes, en diferentes entornos del activo a proteger, de forma que una eventual amenaza pueda ser detectada de forma temprana, se retrase su avance lo máximo posible, y la reacción llegue a tiempo para minimizar su impacto. La defensa en profundidad es claramente uno de los enfoques más efectivos en el control de accesos, como ha venido demostrando en los últimos años la implantación de sistemas de autenticación multifactor [8].

En el ámbito de la protección [9], y dentro del marco operacional [10], el control de accesos es una piedra angular para la defensa de los sistemas. Tal y como se formula en arquitecturas clásicas, como las configuraciones AAA [11], está constituido por las siguientes prácticas:

- Identificación

  Método para sintetizar y codificar, en una primera fase de registro, la identidad de un ente (i.e., valor único e identificativo de una entidad) que interactúa con el sistema de información. Puede ser un simple valor numérico (e.g., id digital), textual, o incluso estar relacionado con una persona física o jurídica (i.e., cualificado [12]). En el marco de ciberseguridad del NIST [9], aunque entra todo dentro de un sólo ámbito (i.e., *"Identity Management and Access Control"*) se diferencia entre gestión de identidades y control de acceso.

- Autenticación

  Mecanismo que permite comprobar que la identidad de una entidad que interactúa con el sistema es la misma que se obtuvo en la fase de registro, facilitada por uno o más parámetros que lo validen a través de [13]:

  - Algo que sabes (e.g., una contraseña)
  - Algo que tienes (e.g., una llave física)
  - Algo que "eres" (e.g., un biométrico)

- Autorización

  Una vez autenticada su identidad, determinar a qué activos puede o no acceder la entidad asociada [14]. Mientras que en este trabajo involucramos los tres componentes de las configuraciones AAA, en algunas referencias, cuando se habla de control de accesos, este se restringe exclusivamente al ámbito de la autorización, con esquemas como:

  - MAC: control de acceso obligatorio (i.e., traducción del inglés *mandatory*), evaluado de forma centralizada
  - DAC: control de acceso discreccional, gestionado por los responsables de cada activo
  - RBAC: control de acceso basado en roles, en lugar de identidades individuales
  - ABAC: control de acceso basado en atributos [15], como la acción a realizar sobre el activo, metainformación del mismo, etc.

- Trazabilidad

  Almacenamiento de eventos, y registro de utilización de recursos por parte del usuario para detectar anomalías y usos indebidos [16]. Esta práctica actúa como puente entre

la protección y la detección, facilitando también la respuesta a las amenazas y la recuperación de los activos.

Aunque el diseño de todas estas prácticas es estático, su uso debe ser dinámico, en base al perfil de riesgo del sistema (e.g., utilizando múltiples factores de autenticación la primera vez que un usuario accede a su correo, y limitándolo a uno cuando se confía en el equipo desde el que accede). Pero el perfil de riesgo también puede variar, por lo que se requiere una seguridad, además de dinámica, adaptativa [17] (e.g., volviendo a pedir otro factor de autenticación si se detectan anomalías, o se va a acceder a un recurso crítico).

La trazabilidad en el uso de los activos se puede explotar para determinar el perfil de riesgo, y establecer estas medidas de forma adaptativa; pero también permitirá, en algunos casos, inferir la identidad del usuario: obtener un perfil biométrico basado en conductas.

Esta biometría conductual puede encajar como un "algo que eres" no determinista a la hora de resolver la identidad de una entidad en aras de autenticarla frente a algún sistema de información (e.g., satisfaciendo diversos parámetros de cara a iniciar sesión [18]). Por sus características (i.e., métodos basados en la observación, y no en la colaboración del usuario) la biometría conductual es un mecanismo de biometría ligera.

Llamaremos autenticación continua, o autenticación activa [19], al uso de sistemas de biometría ligera para asegurar que la identidad de una entidad sigue siendo la legítima a lo largo de una sesión de trabajo, tras el acceso inicial. La autenticación continua puede consistir en la comunicación continua de la identidad obtenida mediante síntesis de diferentes parámetros, o la resolución constante de operaciones que permiten caracterizar dicha identidad [17]; además de en sistemas de análisis de patrones.

Para caracterizar qué sistemas permiten la autenticación continua, y diferenciar cuáles de ellos pueden hacerlo de forma adaptativa, y cuáles no, se ha llevado una revisión sistemática de la literatura. Partiendo de 120 investigaciones, y aplicando diferentes criterios de inclusión y exclusión, se sintetizan las conclusiones de las 30 contribuciones de mayor impacto del momento. Este estudio resulta crucial para el desarrollo de esta tesis, porque permite concretar los elementos y términos de la autenticación continua, y fijar el alcance de una manera objetiva.

Tras este estudio del estado del arte se propone, y evalúa, un sistema de autorización dinámica. De esta forma se concreta una primera medida de protección, basada en los principios de la autenticación continua, para dotar de resistencia al proceso de autenticación para entornos con recursos limitados, o expuestos a adversarios con capacidad de interceptación de las comunicaciones.

Finalmente se analizan las capacidades de diferentes algoritmos de inteligencia artificial a la hora de determinar la identidad del usuario en base a sus patrones de tecleo. Se concluye así abordando directamente la autenticación continua a través de un estudio

que fija una base de conocimiento homogénea que permite comparar estos algoritmos, y validando un sistema para la protección de dispositivos móviles.

1.1.1 Definición del problema

Los sistemas de información pueden ser vulnerables en múltiples niveles. La seguridad en los equipos que actúan como autoridad (por su posición en el sistema de información, o por contener algún activo criptográfico relevante), también puede sufrir fallas (e.g., como evidencia el incidente que sufrió la plataforma de gestión de identidades Okta [20]), por lo que se debe adoptar un enfoque de defensa en profundidad [21] estableciendo medidas de seguridad multinivel; pero también se debe actuar de forma coherente con el nivel de riesgo [22]. Por otro lado, la inclusión de los operadores humanos en el sistema abre la puerta a amenazas derivadas de negligencias, pero también de actuaciones maliciosas que pueden resultar en graves incidentes de seguridad.

Aun contando con sistemas que garanticen una autenticación continua fiable, su aplicabilidad en un sistema de información complejo no es trivial, pudiendo abordarse desde varias perspectivas: entre el sistema de información y un terminal (i.e., autenticando el un equipo local frente a un servidor remoto), entre el terminal y el operador (i.e., autenticando al usuario frente al equipo local), etc.; y no existe una solución única, aun para un mismo caso de uso, cuando cambian parámetros básicos (e.g., un mismo método, basado en analizar el comportamiento del usuario frente al dispositivo, puede no arrojar los mismos resultados cuando el dispositivo es un ordenador, que cuando es un teléfono móvil). Es pertinente analizar qué casos de uso existen, qué algoritmos permiten una mejor interpretación de los registros de actividad para validar la identidad de las entidades legítimas, y cómo se puede responder con eficacia a los riesgos derivados de una suplantación.

En esta tesis doctoral se pretende abordar de qué manera la autenticación continua puede ayudar a mitigar estas amenazas, y cómo puede encajarse en las medidas de protección clásicas para dotarlas de un comportamiento adaptativo en función del nivel de riesgo existente.

Identificamos, con el estudio de la literatura, qué tecnologías permiten la autenticación continua, qué características tienen y qué parámetros las definen como autenticación continua como tal (i.e., qué puede considerarse autenticación continua, en contraste con autenticar continuanmente utilizando un secreto precompartido).

Para abordar la protección de las comunicaciones entre el sistema de información y el terminal, se ha desarrollado mejoras sobre los sistemas clásicos de “port-knocking” que, haciendo uso de autenticación dinámica, permiten evitar suplantaciones por parte de adversarios locales o con capacidad de interceptación.

Como el acceso de un operador al terminal sigue siendo crítico, incluso de cara a proteger el sistema de información remoto (que a priori no cuenta con ningún elemento

para discriminar entre operadores, una vez el terminal está autenticado y autenticándose continuamente), se aborda la protección de este terminal con mediante autenticación continua. Para ello, se estudian diferentes técnicas de tratamiento de datos para autenticar o detectar intrusiones analizando el uso del teclado, con el menor número de eventos posibles.

1.2 Objetivos de investigación

Esta tesis tiene como objetivo general estudiar los sistemas de autenticación continua y valorar su papel en la seguridad de la información desde un enfoque de defensa en profundidad. Persigue también:

1. Caracterizar los sistemas de autenticación continua, identificando características que permitan diferencia los, entre otros, de los sistemas basados en autenticación dinámica clásicos (e.g., OTP)
2. Definir estrategias que potencien la defensa en profundidad de los sistemas clásicos de control de accesos, mediante la aplicación de los princpios de la autenticación continua.
3. Definir bases de conocimiento, que dé apoyo a la toma de decisiones a la hora de implantar sistemas de autenticación continua en un control de accesos.
   (a) Analizar, empíricamente, las capacidades que ofrecen diferentes algoritmos de aprendizaje automático para la autenticación continua basada en biometría conductual, definiendo para qué casos de es más conveniente el uso de cada uno de ellos.

1.3 Estado del arte

La investigación desarrollada por Shepherd en [23], es una de las primeras investigaciones que mencionan el término “autenticación continua”. Partiendo de estudios psicológicos de la biometría implícita en los patrones conductuales, desarrolla un mecanismo que permite distinguir usuarios mediante la medición de características de tecleo. Esta aproximación utiliza exclusivamente estadística descriptiva básica (i.e., media y varianza), pero marca un primer hito por su aplicabilidad a sistemas de información reales.

Los sistemas biométricos clásicos se clasifican en base a los siguientes principios [24]:

- Universalidad

  Son aplicables a cualquier individuo normativo (i.e., no requiere que el individuo tenga ninguna característica especial))

- Singularidad

  Permiten identificar de forma unívoca a un individuo concreto

- Permanencia

  Son propios del individuo, y no variarán con el paso del tiempo

- Colectibilidad

  Su recolección es sencilla, y puede medirse de forma cuantitativa

Sin embargo, como podremos observar, los sistemas de autenticación continua no siempre cumplen con estos parámetros. Muchos se limitan a tratar de proteger una sola sesión de trabajo (i.e., no cumplen con la permanencia), no son deterministas, o se basan en características concretas relacionadas con las habilidades del usuario. Lo que primará es que cumplan con el pincipio de colectibilidad, de cara a que el sistema sea lo menos intrusivo posible, y se mantenga, si no oculto, imperceptible.

Para diferenciar este tipo de biometría no intrusiva, de una biometría clásica: huella dactilar, retina, etc.; mucho más intrusiva a la hora de recolectar la información, se acuña el término "biometría suave" [25], frente a la denominada "biometría dura". Los criterios más aceptados para que un sistema biométrico sea considerado suave son la distancia con la que se puede identificar al sujeto (i.e., desde lejos, sin necesidad de contacto), que no se requiera cooperación o interacción activa, o que no requiera de una fase de registro, sino que se pueda inferir a lo largo de la sesión, por ejemplo, que el color de la camiseta deba ser el mismo desde el principio hasta el final) [26].

Además, se espera que estos nuevos sistemas sean eficientes (i.e., que, incluso desde el punto de vista computacional, no perturben el funcionamiento del proceso protegido) y aceptables (i.e., usables, en consonancia con el no ser invasivos). También se busca que sean efectivos frente a fraude activo, de cara a enfrentar adversarios que tengan capacidad para emular características de un usuario legítimo. Si es sencillo copiar un atributo, como la huella dactilar, el sistema debería contar con herramientas que permitan detectar que, aunque encaja con el patrón correcto, es un fraude [27].

La biometría cuenta con métricas de error propias, similares a las de otras disciplinas (e.g., estadística, *machine learning*, etc.), pero con particularidades relacionadas con el ámbito del control de accesos. Así, las tasas más importantes a la hora de evaluar un sistema son [28]:

- Tasa de Falsa Aceptación (FAR, del inglés *False Acceptance Rate*)

  Equivalente a la tasa de falsos positivos, indica cuántas veces el sistema ha dado por buena una identidad que no lo es

- Tasa de Falso Rechazo (FRR, del inglés *False Rejection Rate*)

Equivalente a la tasa de falsos negativos, representa el número de veces que se denegaría el acceso una identidad legítima

Estas tasas no son fijas, sino que dependen de los ajustes que se hagan en el sistema: si el sistema se flexibiliza, y el umbral con el que se rechaza a los usuarios baja (i.e., se hace más laxo), aumentará la FAR y disminuirá la FRR. La forma más extendida de medir el rendimiento final de un sistema de autenticación biométrica es la tasa en la que ambos errores se igualan [29] (i.e., EER, del inglés *Equal Error Rate*).

Aunque la autenticación continua requiere que FAR sea prácticamente nula [30], existiendo tecnologías fiables en este sentido (e.g., huellas dactilares [31]), uno de los mayores retos en el uso de la biometría es la FRR [32], más aún cuando lo que se persigue es que el sistema de autenticación continua sea lo menos invasivo posible. A la par que se desarrollan los sistemas biométricos duros, y se formaliza su estudio aparecen nuevos estudios que alcanzan tasas muy bajas de rechazo con nuevos periféricos.

En [33] analizan el movimiento del ratón de un ordenador para alcanzar tasas del 2,4649 (FAR) y 2,4614 (FRR). A este se suman otros periféricos, como la cámara; o el análisis de otros patrones de uso del sistema, como el registro de las aplicaciones.

Aunque el reconocimiento facial es un sistema fiable en conciciones óptimas (i.e., suele tener una baja FAR, a costa de empeorar la FRR), las condiciones y el hardware limitan mucho su efectividad como para utilizarse como método principal de autenticación [34]. Sin embargo, el procesado de imágenes faciales sí es un método potente para la autenticación continua: por un lado no es invasivo, no requiere de una acción concreta por parte del usuario, y una vez cribados los posibles usuarios que cuadran con la imagen (i.e., contando con el contexto de la sesión de usuario), es relativamente sencillo encontrar divergencias. Existen numerosas investigaciones en este sentido, que mediante el uso de técnicas de *machine learning* permiten la autenticación continua. Mediante el uso del algoritmo ABC (del inglés *Artificial Bee Colony*) sobre *eigenfaces*, obteniendo una máscara difusa a partir de la cara, en [35] obtienen una precisión del 86,88 %.

Por otro lado, en [36] son capaces de detectar la suplantación de identidad de un usuario en 30s, con un EER del 1 %, mediante el análisis de los movimientos del ojo.

En [37], donde utilizan el término “autenticación activa” como sinónimo de autenticación continua, frente a lo que llaman “autenticación explícita”, combinan el uso de imágenes con el análisis de registros de auditoría para tratar de reducir en la medida de lo posible el número de acciones de autenticación por parte del usuario

Con la irrupción a gran escala de los teléfonos móviles el mapa de riesgo cambia, haciendo que estos activos adquieran mucho más valor tanto para los usuarios como para los ciberdelincuentes [38]. Por lo tanto deben establecerse nuevas medidas de protección que garanticen la seguridad en estos equipos que, ya sea por inercia, o a raíz de la implantación

de políticas (e.g., BYOD [39]), se han integrado como un elemento más dentro de todos los sistemas de información.

Pese a lo que pueda parecer, aunque los principios son los mismos, tanto los periféricos como la forma de interactuar con ellos (e.g., de teclado físico a teclado virtual, que además añade ruido propio del procesamiento del tecleo) han cambiado, y no se puede hacer una traducción directa de los algoritmos de autenticación continua existentes hasta el momento. Las herramientas de análisis y procesamiento de datos (e.g., algoritmos de *machine learning*, librerías de programación, equipos hardware,etc.) también han evolucionado en paralelo, y se apreciará un cambio de paradigma a la hora de procesar los datos, más alejado de la estadística en favor de la algoritmia.

El ámbito más abordado para desarrollar sistemas de autenticación continua sobre teléfonos móviles es la pantalla táctil. Touchalytics [40] es una de las investigaciones más relevantes en este ámbito. En su trabajo, Frank et al. utilizan características gestuales sobre la pantalla de los teléfonos para identificar un cambio de usuario, obteniendo EER de entre el 0 y el 4 %. Analizan también el impacto que tiene el paso del tiempo en la capacidad de su modelo para autenticar a los operadores, y cómo varía el modelo conductual entre sesiones de trabajo..

Una de las peculiaridades del teléfono móvil es que el contexto de trabajo del usuario puede ser mucho más diverso que en un ordenador: e.g., tumbado, corriendo, con diferentes orientaciones de pantalla, etc. En HMOG [41] combinan patrones de movimiento arrojados por los diferentes sensores del teléfono móvil, tales como acelerómetros, o datos de iluminación, de cara a reconocer a los usuarios en distintos escenarios, con métricas de EER del 7,16 % y el 10,05 %, con el usuario caminando y sentado, respectivamente.

La mayor parte de las investigaciones, buscando la usabilidad y la aplicabilidad de sus métodos, utilizan periféricos que son comunes a todos los dispositivos (i.e., teclado y ratón en ordenadores, cámaras, sensores de los teléfonos, etc.), pero algunas aproximaciones hacen uso de periféricos más avanzados. En [42] refuerzan la seguridad de la sesión autenticada mediante patrones del electrocardiograma del usuario. Análogamente, en [43] ofrecen esta misma función mediante la lectura de señales cerebrales obtenidas por espectroscopia.

1.3.1 Otros ámbitos de aplicación

Aunque el grueso de las investigaciones se centran en la autenticación continua de usuarios, al igual que la autenticación, esta no se restringe exclusivamente a validar la autenticidad de las personas, sino que puede actuar con otras entidades. Wang et al. prueban cómo la radiación electromagnética generada por un equipo puede utilizarse como una huella conductual de las mismas [44].

La aplicación de técnicas de autenticación continua en entornos industriales donde la seguridad de los procesos se delega en dispositivos distribuidos puede fomentar la seguridad y ayudar en la detección de anomalías o intrusiones, por ejemplo en entornos IoT, permitiendo la adopción de estas tecnologías en ámbitos donde la seguridad física podría verse afectada ante un incidente lógico [45]. El estudio de qué estrategias y datos, particulares de las máquinas, electrónicos, o lógicos (e.g., registros de auditoría, que no están presentes en un cuerpo humano), permiten establecer patrones conductuales, es una de las tareas más relevantes en el estado del arte actual [46].

1.3.2 Cohesión con el control de acceso, seguridad adaptativa

Si mediante biometría conductual se pueden detectar anomalías en los dispositivos finales, y estos contienen algún tipo de activo que permite el acceso al sistema de información (e.g., claves, ficheros de configuración, etc.), utilizar la autenticación continua para proteger el dispositivo frente a operadores ilegítimos, tiene aplicación directa en el ámbito de la detección de intrusiones mediante sistemas IDS [47].

La aplicación de la autenticación continua en sistemas de tipo EDR (i.e., sistemas de detección y respuesta) redundaría en las capacidades dinámicas para conseguir una seguridad adaptativa [48]. Del mismo modo es posible detectar que un componente del sistema deja de ser confiable, y se debe realizar alguna acción para que vuelva a serlo, o responder a la amenaza. En resumen, la autenticación continua habilita la configuración adaptativa de los sistemas de control de acceso en base a la percepción del riesgo [49].

Retomando la caracterización de los sistemas biométricos, la permanencia del atributo que permite la autenticación continua abre la puerta a que se pueda implantar como un factor de autenticación primaria más, además de como una medida para mantener la seguridad durante la sesión. Un atributo que permita validar la identidad de un ente a lo largo de las sesiones de trabajo puede ser utilizado como sistema *passwordless* de autenticación [50]; aunque también tiene riesgos implícitos que deben ser evaluados y tratados [51], sobre todo relacionados con la privacidad (e.g., un atributo del que el usuario no puede desprenderse, y puede ser evaluado sin su colaboración, abre la puerta a sistemas de seguimiento y control muy efectivos).

En [52] se realiza un extenso estudio de los diferentes problemas que tiene la autenticación continua, analizando el impacto que tienen la elección de parámetros, o de algoritmos de tratamiento, tanto para la privacidad como para el rendimiento del sistema. Proponen la aplicación de tecnologías de mejora de la privacidad (i.e., PET, de *privacy-enhancing technologies* [53]), como el uso de criptografía homomórfica. También inciden en la importancia de la fase de diseño, donde pueden incluirse elementos similares a los utilizados en el almacenamiento seguro de contraseñas (e.g., uso de *salt* criptográfico) para obtener biometría cancelable.

1.4 Contribución

Pese a existir una gran cantidad de trabajos en los que se estudian mecanismos que permiten la autenticación continua, el objetivo general es el de encontrar sistemas más efectivos, o nuevos métodos para obtener biometría conductual. En la literatura apenas se concreta qué papel debe desempeñar este tipo de biometría dentro un sistema de seguridad de la información, más allá de que permite detectar un cambio de identidad en el operador. Para cubrir este espacio se ha realizado un estudio sistemático de la literatura, y se han propuesto dos mecanismos de protección, basados en autenticación continua, para dos ámbitos diferentes: en la validación del dispositivo como elemento del sistema, y en la operación del usuario con el dispositivo. Los artículos asociados a estas investigaciones han sido publicado en medios científicos con revisión por pares, indexados en el *Journal Citation Report*, y se recogen en esta tesis, a modo de compendio, para ilustrar los resultados de investigación obtenidos.

Artículo 1

- Referencia

  Javier Junquera-Sánchez, Carlos Cilleruelo, Luis De-Marcos, José-Javier Martinez-Herráiz, "Access Control beyond Authentication", Security and Communication Networks, vol. 2021, Article ID 8146553, 11 pages, 2021. https://doi.org/10.1155/2021/8146553

- Resumen

  Con la popularización del modelo *Zero Trust*, y frente al modelo de bastionado por segmentos de red, se pone el foco en la protección estricta de cada uno de los equipos terminales como único método válido para proteger el sistema de información, y para ello es imprescindible que los sistemas de control de accesos de dichos dispositivos sean efectivos. Se conoce como autenticación continua al conjunto de técnicas que permiten determinar que la identidad de un usuario legítimo no ha sido alterada (e.g., no hay otro usuario utilizando sus credenciales, o tomando el control de una máquina con la sesión iniciada) tras el proceso de autenticación. En este artículo se persigue la identificación de tecnologías que permiten esta autenticación continua, algoritmos de tratamiento de los datos que permiten sintetizar modelos válidos, y casos de uso; que permiten utilizar este método para mejorar la seguridad de los sistemas de control de acceso. Para ello, se ha desarrollado un análisis sistemático del estado del arte que ha permitido tanto identificar estos elementos, como estudiar cuáles son más efectivos y aplicables; así como los criterios que permiten catalogar los sistemas de autenticación continua.

- Impacto

La revista *Security and Communication Networks*, en la que ha sido publicado este artículo, divulga contenido relacionado con las implementación de medidas de seguridad en redes de comunicación. Según *Web of Science*, tiene un factor de impacto de 1,968, y un índice JCI de 0,430, posicionándose en el Q3 del ránking JCR de 2021, en la categoría "*Computer Science, Information Systems*".

Artículo 2

- Referencia

  Javier Junquera-Sánchez, Carlos Cilleruelo, Luis de-Marcos, José-Javier Martinez-Herráiz, "C-Lock: Local Network Resilient Port Knocking System Based on TOTP", Wireless Communications and Mobile Computing, vol. 2022, Article ID 9153868, 9 pages, 2022. https://doi.org/10.1155/2022/9153868

- Resumen

  El *port-knocking* es una técnica de control de acceso que consiste en la ocultación de un recurso de red hasta que se interactúe secuencialmente, típicamente mediante una conexión, a una serie de puertos predefinidos (i.e., un "golpeo" de dichos puertos), pero cuando un adversario tiene capacidad de interceptación de las comunicaciones esta secuencia queda expuesta tras el primer acceso. En este artículo proponemos un método, basado en el uso de autenticación dinámica mediante TOTP, que permite que la secuencia se actualice periódicamente permitiendo la implementación de la técnica de *port-knocking* en entornos adversos, como pueden ser entornos controlados por un adversario, o redes locales.

- Impacto

  Este artículo ha sido publicado en la revista *Wireless Communications & Mobile Computing*, de la editorial Wiley-Hindawi. Esta revista persigue ser un espacio de divulgación para la comunidad académica y la industria de las tecnologías de infomación y comunicación. Con un factor de impacto de 2,146, y un índice *Journal Citation Index* (JCI) de 0,410, se encuentra, según la web *Web of Science* en el Q3 del ránking *Journal Citation Report* (JCR) de 2021, en la categoría "Computer Science, Information Systems".

Artículo 3

- Referencia

  de-Marcos, Luis, José-Javier Martínez-Herráiz, Javier Junquera-Sánchez, Carlos Cilleruelo, and Carmen Pages-Arévalo. 2021. "Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics" Electronics 10, no. 14: 1622. https://doi.org/10.3390/electronics10141622

- Resumen

  Debido a la exposición que tienen los teléfonos móviles, la autenticación continua esta adquiriendo importancia a la hora de proteger estos activos para mitigar los riesgos derivados de la pérdida o la substracción. Aunque en la literatura existen aproximaciones en las que se consigue la autenticación continua utilizando múltiples fuentes de datos (e.g., sensores, eventos de escritura, gestos en pantalla, u otras interacciones) hay tal diversidad de técnicas y sistemas utilizados para la adquisición y procesamiento de la información, que se hace difícil comparar dichos métodos de una forma fiable. En este estudio se han utilizado datos de escritura con teclado virtual del *dataset* público "HMOG" para entrenar siete clasificadores diferentes, incluyendo métodos de *ensemble* (RFC, ETC, y GBC), supervisados (k-NN y SVM), árboles de decisión (CART), y otros métodos probabilísticos (naive Bayes); mostrando cómo con pocos eventos se puede determinar la identidad de un usuario. Los resultados arrojados por los algoritmos de *ensemble* se muestran superiores a los demás, con una especial preponderancia del algoritmo GBC.

- Impacto

  El artículo ha sido publicado en Electronics, una revista de la editorial MDPI enfocada en la electrónica aplicada, y de lectura gratuita bajo el marco *Open Access*. *Web of Science* la sitúa en el Q2 del JCI del año 2021, en la categoría "*Engineering, Electrical & Electronic*", con un factor de impacto de 2,690.

1.5 Resumen de la contribución

Los tres artículos del compendio contribuyen a la consecución de los objetivos de investigación.

Con el estudio sistemático del estado del arte llevado a cabo en el primer artículo conseguimos cerrar el alcance sobre qué va a formar parte de los sistemas de autenticación continua (i.e., qué debe llevar esta etiqueta, y qué debe llevar otra), así como de los diferentes métodos existentes para procesar la información de cara a que estos sistemas de autenticación continua permitan actuar conforme al riesgo de suplantación.

El segundo artículo identifica una medida de protección de los sistemas de control de acceso mediante sistemas dinámicos, y evidencia que, en contraste con la definición de [17], los sistemas basados en secretos precompartidos no ofrecen las mismas garantías adaptativas, y sus capacidades de autenticación continua no están al mismo nivel que las de los sistemas basados en biometría conductual.

Finalmente, el segundo artículo complementa los resultados del primero, y permite alcanzar el objetivo de investigación 3a, evaluando de forma experimental diferentes al-

goritmos de clasificación para, mediante patrones de tecleo, modelar la identidad de un usuario, y proteger un terminal móvil.

La Tabla 1.1 expone la relación entre los artículos presentados y los objetivos de investigación (OI), indicando si contribuye total (T) o parcialmente (P) a su consecución.

Artículo	OI1	OI2	OI3	OI3a
Art. 1. Access Control beyond Authentication	T	-	P	-
Art. 2. C-Lock: Local Network Resilient Port Knocking System Based on TOTP	P	T	-	-
Art. 3. Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics	-	-	P	T

Tabla 1.1: Relación entre artículos y objetivos de investigación.

1.6 Estructura

Esta tesis presenta la siguiente estructura:

El Capítulo 2 muestra el estudio sistemático del estado del arte llevado a cabo para cerrar el contexto de la autenticación continua e identificar los distintos componentes (i.e., fuentes de información, mecanismos de procesado, respuesta, etc.) que permitan integrar la autenticación continua, de manera exitosa, en los sistemas de control de acceso existentes.

El Capítulo 3 presenta el segundo artículo del compendio, en el que se propone un sistema de autenticación dinámica para la protección de las comunicaciones entre un terminal y un servidor. Este artículo evidencia que no cualquier sistema dinámico responde a los requisitos de la autenticación continua, y abre la puerta a profundizar en estos últimos de cara a lograr los objetivos de la tesis.

El Capítulo 4 expone el tercer y último artículo del compendio, en el que se evalúan diferentes algoritmos de procesamiento para modelar, en base a los patrones de tecleo en un teléfono móvil, la identidad de los usuarios. Por un lado es un estudio metódico que ayuda a identificar qué algoritmos son más efectivos a la hora de evaluar el riesgo al que está expuesto el sistema (i.e., desde el punto de vista de la suplantación de identidad), y por otro sirve como clausura, en coalición con el segundo artículo presentado en el Capítulo 3, con respecto a la protección de los sistemas de control de acceso.

Los capítulos 5 y 6 desarrollarán, respectivamente, la discusión de los resultados y las conclusiones del trabajo.

Capítulo 2

Revisión sistemática de la literatura sobre autenticación continua

2.1 Contribución del artículo 1

Los modelos clásicos de seguridad en los sistemas de información se han basado siempre en la creación de perímetros de seguridad en los que cada uno de los activos, y sus operadores, son confiables una vez validada su identidad en el proceso de autenticación. Pero con la difusión de los entornos distribuidos, con perímetros cada vez más difusos, se extiende el modelo Zero Trust: un paradigma de protección de los sistemas de información en el que se transfiere a cada uno de los activos del sistema la responsabilidad de autenticar cada una de sus interacciones con el resto de los dispositivos, y con los usuarios operadores. Sin embargo existen escenarios en los que los procesos de autenticación, que normalmente se producen al principio de la sesión de trabajo, no garantizan que la identidad del operador no sea suplantada: e.g., robo del dispositivo, ausentarse del puesto de trabajo con la sesión desbloqueada, filtración de credenciales, etc.; y repetir periódicamente el proceso de autenticación puede resultar molesto para el usuario, con la consecuente merma en la usabilidad del sistema.

La autenticación continua busca cubrir esta necesidad mediante la implantación de procesos de autenticación en los que el usuario no tiene que participar activamente; pero la ingente cantidad de fuentes de información, algoritmos de procesamiento de dicha información, y métricas que permiten medir su efectividad en el proceso de validación la identidad del usuario, dificultan su implantación efectiva como medidas de protección de los sistemas de información. Además, se encuentra en la literatura una ausencia de criterio a la hora de determinar si una tecnología pertenece o no al ámbito de la autenticación continua, llegando denominarse así sistemas que no cumplen con los requisitos previamente enunciados (i.e., sistemas adaptativos que no requieren la participación activa del usuario en el proceso de autenticación). Es por esto que se hace necesario realizar un estudio que

fije las bases para introducir la autenticación continua en las prácticas de securización de los sistemas de información.

En este capítulo se realiza un estudio sistemático de la literatura en el que se trata de enumerar ámbitos de aplicación, tecnologías involucradas y métodos de tratamiento de los datos recolectados para conseguir la autenticación continua. Se ha optado por este enfoque sistemático porque, al margen de los problemas comentados con los criterios de enmarcación de la autenticación continua, en el momento de su realización estaban comenzando a popularizarse sistemas comerciales de protección de equipos (e.g., los sistemas subyacentes a las tecnologías EDR y XDR [54]), que si bien podían ser útiles en el ámbito industrial, no contaban con elementos que permitiesen evaluarlos con suficiente objetividad (e.g., revisión por pares, libros blancos, etc.); y era imperativo contar con criterios claros de inclusión y exclusión de las fuentes documentales.

2.2 Artículo 1

A continuación se expone el artículo 1 del compendio, "*Access Control beyond Authentication*".

Hindawi
Security and Communication Networks
Volume 2021, Article ID 8146553, 11 pages
https://doi.org/10.1155/2021/8146553

Research Article

Access Control beyond Authentication

Javier Junquera-Sánchez, Carlos Cilleruelo, Luis De-Marcos, and José-Javier Martinez-Herráiz

Computer Science Department, University of Alcalá, Alcalá, Spain

Correspondence should be addressed to Carlos Cilleruelo; carlos.cilleruelo@uah.es

Received 3 June 2021; Revised 30 July 2021; Accepted 7 September 2021; Published 1 October 2021

Academic Editor: Luigi Catuogno

Nowadays, the Zero Trust model has become one of the standard security models. This paradigm stipulates as mandatory the protection of each endpoint, looking for providing security to all the network. To meet this end, it is necessary to guarantee the integrity of the access control systems. One possibility for bringing security to the different endpoints is continuous authentication, as an access control system. Continuous authentication is the set of technologies capable of determining if a user's identity remains in time; whether he is the legitimate user (i.e., the only one who should know the secret credentials) or the identity has been impersonated by someone else after the authentication's process was completed. Continuous authentication does not require the active participation of the user. Aiming to identify the different technologies involved in continuous authentication's implementations, evaluation methods, and its use cases, this paper presents a systematic review that synthesizes the state of the art. This review is conducted to get a picture about which data sources could allow continuous authentication, in which systems it has been successfully implemented, and which are the most adequate ways to process the data. This review also identifies the defining dimensions of continuous authentication systems.

1. Introduction

The increase in the use of mobile devices with access to critical resources also increases the possible attack surface of digital assets. A mobile phone or laptop can now be a possible entry point to a private company's network or data. These devices can easily be stolen or accidentally left unlocked and unattended.

Taking this into account, the classic model based on well-defined perimeter security policies is no longer effective [1]. It is also necessary to highlight elements such as the cloud that redefines perimeters with new architectures and interconnections between systems. The security paradigm based on a Zero Trust model [2] now demands new designs of the methodology in security protection and information access for each system. Under the umbrella of endpoint detection and response technologies [3], continuous authentication (CA) aims to ensure that only authorized users interact with the system.

1.1. A Systematic Literature Review Necessity. An effective way to continuously identify a user is by the analysis of the interactions with a device. Even though every interaction with a device may produce a digital fingerprint [4] (behavioural biometric), it is not easy to determine how many different interactions exist and how many of them are required to uniquely identify a user. Determining which continuous authentication technologies exist and are effective facilitates new research that avoids replication and focuses on unexplored areas. Similarly, practitioners and system developers can focus on proven approaches for their implementations of CA solutions.

A systematic review is also convenient to get acquainted with the terminology, common parameters, and techniques used in this research field. These are useful to make future results more accessible to the scientific community and allow research papers to be more homogeneous and accessible. An unbiased systematic review also points to the most relevant research results in the field, and it is an initial point for

researchers in the area [5]. This paper also aims to provide a taxonomy of existing CA approaches. Finally, this SLR identifies the limitations of current systems and the boundaries of CA as a research field, offering guidance for future research. The remainder of this paper is structured as follows. The Background section documents the principles of continuous authentication as well as the concept of Systematic Literature Review (SLR). Methodology section explains the methodology followed to perform the review. One of the objectives of this paper is to perform the literature review with the fewer biases possible, so this section is fundamental. Search Strategies section states the definition of different search strategies that will be used to provide the studies to review. Findings section presents a purely technical analysis of the research studies (i.e., just documenting the elements which fit into the defined methodology). Discussion section contains how the findings, documented in the Findings section, shape the state of the art in CA and the gaps that can be approached in future works. Finally, the Conclusions section provides concluding remarks of the paper. The materials produced to support the research process, and for structuring the documentation of the review, are provided as supplementary material (available here).

2. Background

2.1. Systematic Literature Review. A Systematic Literature Review (SLR) is a method of study focused on synthesizing all possible information about a specific research field. An SLR will be conducted through identification, selection, and evaluation of the state of the art [6].

2.2. Continuous Authentication. Continuous authentication (CA) could be defined, within an access control system, as a new stage of authentication after the initial authentication has been completed, allowing for validation of a user or users during the session [7]. Checking if the users are who they claim to be during their session, it allows for further protection of information assets and also facilitates detecting stolen credentials or other authentication information.

To achieve CA, it is necessary to study the techniques that a machine can use to identify a user (i.e., which technologies allow to retrieve enough information to distinguish every single user). CA systems can be divided into two main families based on the capabilities they have for identifying the entity under evaluation:

(i) Session-based CA systems: the reliability of these systems are determined by the capacity to determine if the entity that is being evaluated has changed or is still the same during the session. For example, a system will be able to identify if the person who initiates a session is the same or if during this session changes. These systems should have a low False Rejection Rate (FRR).

(ii) CA systems based on behavioral fingerprint: these systems can process more information about the entity under evaluation. They can produce a digital fingerprint of users, in the same manner as a classical fingerprint is used to identify a person. The accuracy of these systems is based on their capacity for telling apart a user from the other users. These types of systems should present a False Acceptance Rate (FAR) close to zero.

On the other hand, based on the parameters collected to create these systems, it is possible to differentiate between.

(iii) Hard biometrics (intersession): the biometric data does not change throughout the period that the system is active. However, this group could also include biometric data that only changes slightly or remains the same during long periods of time.

(iv) Soft biometrics (intrasession): soft biometrics are biometric data that will only be valid for a few weeks or days during a session, for example, the colour of a t-shirt.

As shown in Figure 1, these two dimensions determine the potential applications of a continuous authentication system. However, it is necessary to understand having a passive nature (i.e., not interrupting or interfering with the user's tasks) is considered a viability requirement for any CA approach.

Even though the most obvious application of these systems is the ones authenticating human users, it is also necessary to consider that they can be applied to other different entities (e.g., to authenticate devices in an IoT-based smart grid [8]).

3. Methodology

This SLR was divided into three stages: method definition, document compilation, and analysis of the documents and synthesis of results. To accomplish our objective (i.e., developing a rigorous literature study), we followed up the methodology proposed by Arksey and O'Malley [9]. This methodology is divided into the following five stages:

(1) Identifying the research questions

(2) Identifying relevant studies

(3) Selecting studies based on well-defined criteria

(4) Extracting relevant data in a structured manner

(5) Analyze the data and extract results

Across this section, the first three stages as well as the research questions are described in detail. And, later on, the Search Strategies section provides further details of the specific details of the Method Definition. Results are also presented in a separate section.

3.1. Method Definition. The definition of the method to conduct the analysis includes the following steps:

(1) Research questions: determining the questions that are relevant for getting a picture of the state of the art of CA systems.

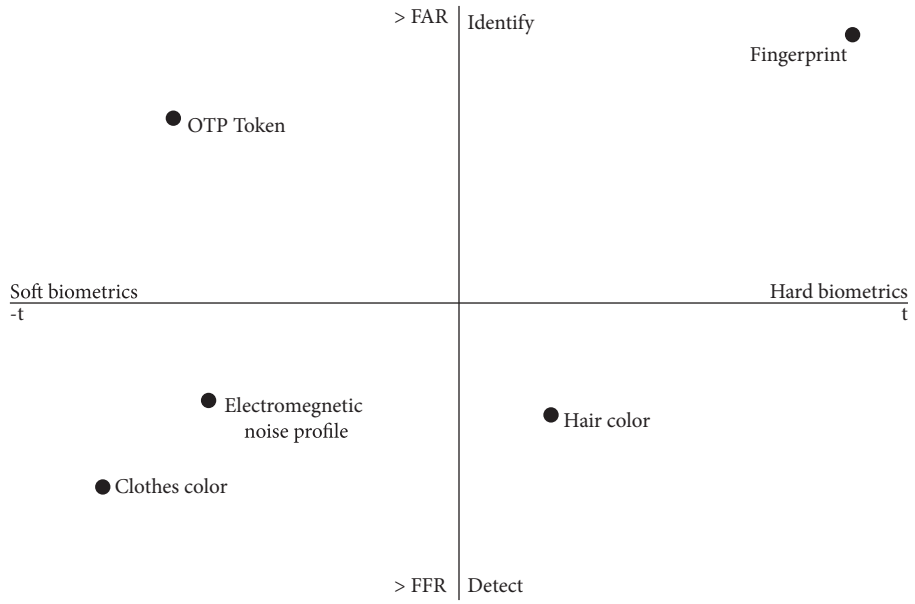

Figure 1: Permanence/distinctiveness map in continuous authentication.

(2) Identifying search strategies including the keywords and sources: the aim is that the search can be replicated.

(3) Identifying inclusion/exclusion criteria: An objective evaluation process must be defined to determine which results fit the SLR goals or, at least, which provide enough information to answer the research questions. Also, the analysis seeks to avoid biases derived from secondary research works. In this phase, a list of criteria is defined to decide the inclusion or exclusion of search results.

(4) Quality Evaluation Strategy: defining the quality criteria that the studies must meet to be included in the study.

(5) Data Extraction Strategy: determining how the data of the studies will be collected so that it can be used to address the research questions.

(6) Elaboration of supporting materials: building supporting evidence (tables, forms, etc.) that facilitates understanding the results and provide evidence to ensure the integrity of the process and its results.

3.2. Document Compilation. The compilation of documents comprised three steps:

(1) Search in data sources: the 20 most cited of each of the data sources are selected.

(2) Metadata extraction: title, authors, number of pages, etc.

(3) Selection based on inclusion/exclusion criteria: initial filtering based on the abstract to remove unrelated studies was followed by a quick inspection to determine if the remaining studies meet the inclusion/exclusion criteria.

3.3. Analysis of the Studies. Document compilation was followed by an analysis of the research studied following the next steps:

(1) Due to the volume of data that a complete analysis requires, the 80 papers (20 results of 6 different sources) were studied in three iterations using the following approach:

  (a) The first three papers from each source were used to create a first picture of the state of the art.
  (b) Up to 5 papers were then added to complete state of the art.
  (c) If the new papers (second step) changed substantially the results we get from the first step, the following studies of search results would also be analyzed, up to 10 per source. We set the limit to 10 because after applying the inclusion/exclusion criteria on the search results because the sample to be analyzed can be different for each source.

(2) Instead of evaluating the studies returned by each source in turn, one study from each source was selected each time. Thus, if there were 5 different data sources, every 5 research papers studied would include one paper from each source.

  To detect coding errors, each time a paper was analyzed, the reviewer name was included, and the evaluation status was updated in a common document used by all the reviewers.

(3) Determining the research questions that each research study addresses.

(4) Developing the data extraction strategy, taking into account that if at this moment it was found that any study did not meet the inclusion criteria or the quality, it would be removed and the decision was recorded.

(5) Analysis of results: when all data (i.e., the elements defined by this procedure) was extracted from original sources, it was analyzed and presented as answers to the research questions in the form of an R/RQ matrix to synthesize the state of the art.

3.4. Research Questions (RQ). In this work, we aim to synthesize the state of the art of CA by analyzing how relevant existing studies address the following research questions. Questions with an identifier are available in the Supplementary Material (see Table of Selected Papers, Results of the Search, and Research Questions):

(i) RQ1: which information allows to perform continuous authentication?

(ii) RQ2: how is data obtained?

(1) RQ2.a: what mechanisms are used to obtain data? Which procedures, devices, or combination of devices enables data collection for CA (e.g., capturing heart activity could be done through electrocardiography or using a microphone)?

(2) RQ2.b: what characterizes the data (e.g., the feature extracted to characterize the heart activity could be the distance between frequency peaks, a wavelet spectrum, etc.)?

(iii) RQ3: what mechanisms are used to process this data?

(1) RQ3.a: how is the data synthesized? How is the data encoded for subsequent processing? What parameters are extracted to generate a digital model?

(2) RQ3.b: how is the decision model built? How a decision model is generated and how it defines the identity of the user (e.g., machine learning and statistics)?

(iv) RQ4: how can CA be integrated into an access control system?

(1) RQ4.a: how does it react in case of an incident detection? Given that the ideal is that the system never disturbs the work of a legitimate user, how does the access control system act if the CA system fails to authenticate the user?
What is the most reliable way to achieve this, taking into account the capabilities that an attacker with access to the machine can have?

(2) RQ4.b: how different models can be combined to produce greater accuracy?
What combinations of systems can offer a more reliable result, and how they can be combined?

(v) RQ5: where can continuous authentication be applied?
In which fields or on which systems can continuous authentication be a contribution?

(vi) RQ6: is it possible to generate a unique fingerprint? Or is it only possible to verify if what is on the other side remains to be the same?

(1) RQ6.a: what hard biometric systems exist? What features, regardless of the accuracy of the systems, will be representative of the actor life?

(2) RQ6.b: what soft biometrics systems exist? What elements are usually part of the identity of the actor, and therefore, allow their recognition throughout (at least) one session?

An example of a piece of research that answers all the questions is the following:

We will authenticate people through the typing of text peculiarities (RQ1). Through the camera (RQ2.a), we will analyze the hand position each time keyboard shortcuts are used (RQ2.b). Furthermore, we will record the posture of the hand when someone types and the distance between your fingers (RQ3.a). This information will allow us to generate a model using OpenCV (RQ3.b). Having these data sources, it is possible to contrast the typing speed captured by the camera with the speed at which the keys enter the system (RQ4.b), and if the system fails, we will request authentication again (RQ4.a). Given that according to the results of the research, each user types in a unique way (RQ6 and RQ6.a), we could implement this in all offices so that users do not have to block their equipment when they go out for lunch (RQ5).

4. Search Strategies

This section details the most important steps of the method definition stage introduced in the previous section. It describes the search strategy, inclusion and exclusion criteria, quality evaluation strategy, and data extraction strategy.

4.1. Data Sources. The search was carried out using the engines provided by the following sources:

(i) Google Scholar (https://scholar.google.com/)

(ii) ACM Digital Library (https://dl.acm.org/)

(iii) IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp)

(iv) SpringerLink (https://link.springer.com/)

(v) ScienceDirect (https://www.sciencedirect.com/)

(vi) ArXiv.org (https://arxiv.org/)

4.2. Study Categories. As long as they meet the inclusion criteria and quality criteria, this SLR considered the three following types of studies:

(i) Papers

(ii) Patents

(iii) Nonacademic white papers

4.3. Search Terms and Results Storage. To find research papers related to continuous authentication, the search term used was "continuous authentication." Furthermore,

advanced search options were configured to search in the abstract, when the search engine has this option or on the full text otherwise (e.g., ACM Digital Library has the option of searching within the abstract, but in Google Scholar we had to set up the search to find the terms "anywhere in the article"). The first 20 search results from each source, ordered by the number of citations can be found in the Supplementary Material.

4.4. Inclusion and Exclusion Criteria. All the results obtained in the data sources were saved, but only studies that met the following criteria were analyzed:

(i) Primary research: only primary research was included. Secondary sources such as reviews or studies of the state of the art were not included.

(ii) No posters: although they may be useful to complement this, posters usually do not provide enough information to build a solid analysis and may generate biases when interpreting results.

(iii) No duplicates: when two data sources return the same result, the second instance is removed.

(iv) English-only papers: as English is the language used for scientific communication [10].

(v) Research papers that, even using the search term "continuous authentication," do not fit our definition were excluded. Examples of this case include the following:

  (i) Papers addressing how to use an authentication factor repetitively
  (ii) Studies focusing on data validation instead of entities
  (iii) Studies based exclusively on classical authentication (tokens)

(vi) All the papers must be published in peer-reviewed sources

4.5. Quality Evaluation Strategy. The quality of each study for this SLR was assessed in terms of the following criteria:

(i) It includes experimentation.

(ii) It uses public datasets that enable replicating the results.

(iii) The performance is over 70% for at least one of the target metrics.

(iv) Simplicity: it is easy to validate the results, and it is a method that can be implemented in other systems. To measure the complexity of the solution, from 1 to 5 (being 1 very simple and 5 very complex), we use the following scale:

  (1) Reads logs from the system
  (2) It is necessary to run a specific software
  (3) It is necessary to use a common IO device (e.g., webcam and mouse)
  (4) It requires a specific IO device (e.g., brainwave sensor)
  (5) Requires that the user follows a specific task (e.g., do a task which is not part of his activity with the system)

(v) The study contains enough information to reproduce the experiment

(vi) Number of different evaluation methods

(vii) Number of research questions addressed

Those studies, which meet at least half of these quality criteria and address at least three research questions, were included in this SLR. Studies not meeting the criteria were excluded and recorded.

4.6. Data Extraction Strategy. The final step before analysis and synthesis is to define a systematic method to extract and code the data from the studies.

4.6.1. Research Questions. An R/RQ matrix relates each study with the research questions that it addresses.

4.6.2. Metadata. The following metadata was gathered for each study: title, authors (only the two first ones), publication date, venue (journal, conference, etc.), type (paper, conference, book, or patent), and number of pages.

4.6.3. CA Data. The following data was gathered for each study about CA:

(i) Entities involved: people, machines, and other

(ii) Data source studied (RQ1)

(iii) Device of the CA system (e.g., mobile and computer) (RQ2.a)

(iv) IO method to obtain the user's data (e.g., camera and keyboard) (RQ2.a)

(v) What makes the input data useful to perform continuous authentication? (i.e., which peculiarities does this data have that allows identifying a user?) (I) (RQ2.b)

(vi) How is the model built? (S) (RQ3.a)

(vii) Evaluation method (P) (RQ3.b)

(viii) Type of continuous authentication (RQ6): the quadrant that best identifies the approach from Figure 1 (permanence/distinctiveness ratio).

(ix) System applications (RQ5)

(x) Is there any kind of experimentation reported in the research?

(xi) If there is experimentation, what is the size of the population?

(xii) Is there a public dataset? (RQ2)

(xiii) What is the reported performance of the research results?

(xiv) Is the method reproducible?

(xv) From 1 to 5, how complex is the solution?

(1) Reads system logs
(2) Develops a program that evaluates user behaviour
(3) Requires a specific IO device/method, but it is common
(4) Requires a specific unusual IO device/method
(5) Requires that the users modify the way they work

(xvi) Comments

4.6.4. Support Documents. Supporting documents included tables to save the search results and the data extracted, tables to check each inclusion/exclusion criteria for each study, and the R/RQ matrix to determine the relationship between studies (R) and research questions (RQ). The data extraction strategy of elements related to continuous authentication was coded using Google Drive survey.

5. Findings

5.1. Process Findings. This section summarizes the main findings of the literature review. The complete table of selected papers, search results, and research questions are included as supplementary material (see Table of Selected Papers, Results of the Search, and Research Questions).

5.2. Selected Primary Research Works. 84 papers of the initial 122 met the inclusion criteria. 38 were removed for the following reasons:

(i) 26 did not meet inclusion/exclusion criteria

(ii) 5 documents were not accessible

(iii) 7 duplicated

Of all these papers, 30 studies were included in the first two iterations of the analysis. The complete list can be found under the "Selection of Articles" sheet of the Supplementary Material (see Table of Selected Papers, Results of the Search, and Research Questions). Three of them were also removed after checking the quality criteria as follows:

(1) Two papers met exclusion criteria:

(i) Not fitting with the focus of this study (R028, [11]).
(ii) It is considered a secondary research work for the purpose of this review. Its objectives are to develop an adversary modelling system (R086 [12]).

(2) One paper did not contain enough information to be able to assess and rate (R044 [13])

6. Results of the Research

After evaluating the remaining 30 documents and carrying out the data extraction process, we found the following results.

6.1. R/RQ Relationship. While the vast majority of studies document the entire characterization and modelling process of the actor for authenticating this character, very few fit it into an access control system or propose a system to be able to contrast the results of their method with other authenticator.

When determining the position of the solution in the permanence/distinctiveness, Figure 1, only a few studies gave a clear answer or the authors did not address the problem in a similar dimension, despite using the same indicators when focusing the study (R027, [14]).

The "RQs" Table 1 presents the matrix of the relationship between the research questions and the research studies that address them. The complete detailed table can be found in the Supplementary Material (see).

6.2. Technologies Evaluated. Almost all of the 30 research studies included in this review analyzed methods to authenticate people, except one (R085, [15]) that presents a method to authenticate machines through the analysis of the electromagnetic radiation they produce. The relationships between the technologies used are presented in Figure 2.

Along this work, we identified that 40% of the studies used mobile phones to authenticate users, contrasting with the 13% focusing on computers. Only one of the previously analyzed research studies explicitly applies continuous authentication to both, mobile phones and computers, and just one aims to perform continuous authentication on smart glasses (R066, [16]). The remaining studies do not explicitly indicate if authentication takes place on any specific device, but they describe different use cases, such as authenticating drivers who get in and out of the vehicle (carriers) or monitoring workstations (which could be associated mainly with desktop computers).

The main IO methods used to get data from the actor to be authenticated are

(i) Touch screen: most used to collect characteristic gestures of a user, but also as a method to input text through different typing methods

(ii) Mobile phone sensors: the accelerometer, gyroscope, or magnetometer of the phone are often used to complement other measures, in the context of the user activity; although sensor information can also be used on its own to characterize user patterns (R005, [17]).

(iii) Camera: mainly through facial recognition and evaluation of other session observable characteristics such as clothing, hair colour, and glasses

(iv) Keyboard and mouse: patterns of use of both devices, present in all computers (also through soft-keyboards in mobile phones), can also be used to identify or complement user modelling

We also found two CA research studies that analyze brain activity (R045, [18]; R063, [19]). Their implementation is rather complex requiring specific hardware and working conditions. In terms of hardware requirements, the only

Table 1: R/RQ relationship.

Code	R001	R005	R006	R007	R008	R023	R027	R028	R030	R031	R045	R046	R048	R049	R063	R065	R066	R068	R069	R083	R084	R085	R087	R104	R106	R107	R109	R110	R113
RQ1	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ2	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓
RQ2.a	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓
RQ2.b	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓
RQ3	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ3.a	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓
RQ3.b	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓
RQ4	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
RQ4.a	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
RQ4.b	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗
RQ5	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓
RQ6	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✓
RQ6.a	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✓
RQ6.b	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓

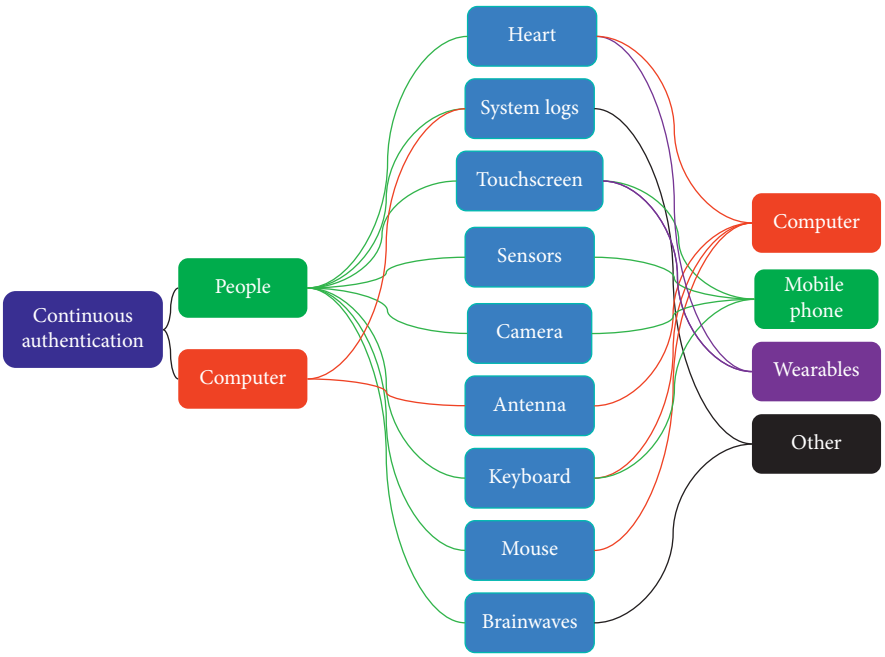

Figure 2: Continuous authentication components' relationship.

other exception was R023 [20], which required a special camera. The rest of the studies can be put in practice in common existing environments and devices, requiring only in a few cases to have access to system logs.

6.3. Data Processing Approaches. We found the following artificial intelligence algorithms in the studies analyzed as part of this SLR:

(i) Support Vector Machine (SVM): it is one of the most used classification techniques, and 10 of the 30 research papers analyzed use SVM. Depending on the type of samples of the dataset, different SVM can be used:

  (i) Canonical SVM when there are at least two sets of data, SVM can be applied to differentiate the values generated by the genuine actor from the other possible values generated by others. If we had data from 100 users, we could generate a model that would allow us to differentiate one of them from the remaining 99.
  (ii) One-class SVM when there is only one dataset: if there is only legitimate user data and a system wants to classify new data as similar or different.

(ii) k-nearest neighbours: this algorithm groups and classifies new instances by comparing them to their closest k data entries of the existing dataset.

(iii) Eigenfaces is a method for facial recognition based on the reduction of facial images to a series of characteristic vectors. This method generates a facial base model (see Figure 3), called F, and stores the identity of each user and the variation with respect to F for reconstructing the face model later.

Figure 3: Example of eigenfaces' models [29].

(iv) Interactive Artificial Bee Colony (IABC): in R046 [21] research, IABC is used as a method for optimizing eigenfaces. It simulates the behaviour of a bee colony searching for natural resources.

(v) Artificial Neural Network (ANN): this method combines and connects a set of simpler decision-making systems, simulating the behavior of neurons, to recognize patterns (R065, [22]; R049, [23]).

(vi) State-Space Models: one of the simplest ways to approach a classification problem is to model it as a state diagram (as in the case of R109, [24]). Examples of other state-space models include decision trees (DT), Random Forests Classifiers (RFC) (R084, [25]), or decision models based on Markov processes, such as Markov Chains or Hidden Markov Models (R049, [23]; R113, [26]).

(vii) Other probabilistic models: R084 [25] compares different methods including logistic regression and Bayesian classifiers (Naive Bayes). R048 [27] and R110 [28] use simple statistical models.

6.4. Experimentation. All the studies analyzed in this review included practical experimentation with users. The average sample is 58.75 subjects.

6.5. Rating Metrics. The following metrics were used to evaluate the quality of the results of the CA systems presented in the studies that are part of this SLR:

(i) False Acceptance Rate (FAR): it measures the percentage of identification instances in which illegitimate users are incorrectly accepted as authorized users.

(ii) False Rejection Rate (FRR): it measures the percentage of identification instances in which authorized users are incorrectly rejected as illegitimate users.

(iii) Equal Error Rate (EER): it is the minimum point at which FAR and FRR meet. It is a measure of the global effects of the system considering both incorrectly accepted and incorrectly rejected instances. If this rate exceeds 50%, the system performs worse than a random classifier.

The EER achived by R109 [24] is between 34% and 49%, but no other papers show an average EER value higher to 30%.

6.6. A Taxonomy for Continuous Authentication. Figure 4 shows that although most of the systems create reliable and permanent models of users, none manages to create a unique behavioral fingerprint of each user. The absence of systems based exclusively on CA may be because such a system does not contribute substantially to the security of assets. Continuous authentication systems could be a great addition, in terms of accuracy, to other approaches (such as the use of light biometrics in R046, [21]).

Results then suggest that our initial bidimensional model for characterizing users in terms of permanence/distinctiveness is appropriate. R027 [14] presents a four-dimensional model for CA methods:

(i) Universality: whether it can be used with all actors of the population targeted by the methods.

(ii) Distinctiveness: to what extend the method tells apart the individual from the population; it can tell whether the actor evaluated is *X* or is Y, or only can determine "you were *X*, and you are not *X* anymore."

(iii) Permanence: for how long the model produced is valid without requiring new training or rebuilding, that is, how long the actor's behavior (fingerprint) does not change.

(iv) Collectibility: the features allow CA data to be gathered and encoded. They must be quantitatively measurable.

Further, R084 [25] introduces the following additional dimensions:

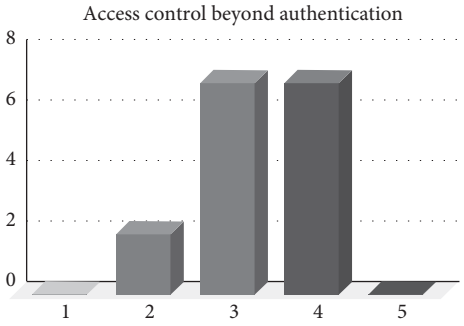

Figure 4: CA system type (1: session CA; 5: behavioral fingerprint CA).

(v) Efficiency: if the system involves mobile phones, which are devices with limited resources, with autonomy that depends on battery consumption.

(vi) Acceptability: determines the level of invasiveness in the user's environment of the CA method.

(vii) Mocking rate: unlike the error rates, the mockery rate measures the effectiveness of the CA system for preventing attacks that falsely recreate the identity of the legitimate user.

7. Discussion

EER is the most common metric to evaluate CA systems. In contrast with machine learning research, where classification is usually measured in terms of positive or negative results (false positives and false negatives), CA results are expressed in terms of acceptance and rejection rates (FAR and FRR). Only the terminology is different, emphasizing the nature of CA as a method for access control.

In quantitative terms, any CA approach with an EER around 30% is considered acceptable, while the best state of the art results report EERs below 10%. Although these EER values are reasonably good (i.e., allow the CA system to work as it should), it must be taken into account that their results are circumscribed to very specific experimental conditions.

HMOG [17] plays a central role in current CA literature, both as holistic research in mobile CA and as a source for further research through its public dataset.

7.1. CA Literature Gaps. This review delimitates the boundaries of CA research. The majority of studies are circumscribed to very specific conditions, sometimes in laboratories, and they do not address the possible consequences of changing the scope to a real-life scenario (i.e., how could it impact model availability). Further, a closer analysis of CA studies that are specific for mobile environments shows that several of them may be difficult to implement in current devices because of technical limitations, such as APIs collecting all user interactions. Approaches such as Touchalytics [30] can only be implemented in a closed run environment with a given application.

Further analysis is also required to determine the features that sustain the initial hypothesis of what CA

approaches can do. Finding new behavioural patterns would mean identifying new methods for CA.

There is still room for improvement and a long way to go until CA systems can generate a unique and durable fingerprint that facilitates noninvasive ways of authentication. Only three of the studies reviewed here [20, 26, 30] consider the possible intersession changes in user models.

Finally, the second iteration of this SLR did not make any substantial changes to the results of the first iteration although it provided more studies that extended and completed the initial analysis. The second iteration did not provide any new use cases scenarios or the involvement of new devices. However, it is necessary to mention that this iteration shows the increased dominance of mobile phones, as the most important target use case for CA research.

8. Conclusions

This paper presents a systematic literature review of CA. After an initial search that returned 120 studies, the 30 most cited papers that met the inclusion criteria took part in the next stage of the study. Results of our review reveal the existing technologies and methods for CA as well as their current limitations. We described the behavioural features used for CA and the techniques to extract and process them. We also describe the main measures used to evaluate the performance of CA systems. Finally, this study also suggests a taxonomy to categorize CA approaches.

This review also describes current trends for CA and the expected levels of performance required for CA systems. Additionally, we suggest the limitations of the existing state of the art for CA research, which may act as a guide for the direction of future research articles. Finally, this review also identifies several research gaps in the CA field, outlining other different lines for new contributions.

8.1. Future Work. Existing research on CA not only shows its impact on the protection of existing systems but also shows that there is still room for new studies, particularly in the line of long-term CA technologies. In what follows, we suggest a few of them.

The fingerprinting aspect (i.e., the possibility of generating a behavioral fingerprint, easy and discreetly to obtain, and from which the user cannot detach itself) also arises the need for studying its ethical impact. Addressing an evaluation from an ethical point of view could be useful to mitigate the impact of these approaches on the privacy of personal data.

Further, the possibility of applying identity analysis systems to other nonhuman actors (e.g., such as the authentication between machines shown in (R085, [15])) opens the door for its use in securing industrial or IoT-related environments.

Finally, due to the character of the review, several novel approaches or commercial products have not been taken into account. Developing a less formal scientifically grounded search method could lead to discovering additional areas or applications of CA.

Data Availability

The data in table used to support the findings of this study are included within the supplementary information file(s).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was supported by the European Union's Horizon 2020 Research and Innovation Program under grant agreement no. 826284 (ProTego).

Supplementary Materials

The materials produced to support the research process, and for structuring the documentation of the review, are provided as supplementary material. The file "Appendix A. Search results (en).pdf" contains a list of all the papers indexed in the early stages of the research. For each one, the columns represent the following: (1) Origin: search engine source; (2) Code: internal code to identify the paper across different support files; (3) Title; (4) Authors; (5) Publishing date; (6) Where: publication name; (7) Type of publication: e.g., journal, conference; (8) Included: checkbox to indicate if the paper becomes included in our review; (9) Pages: length (i.e., the amount of pages) of the paper; (10) Annotations: internal notes. (*Supplementary Materials*)

References

[1] C. DeCusatis, P. Liengtiraphan, S. Anthony, and M. Pinelli, "Implementing zero Trust cloud networks with transport access control and first packet authentication," in *Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 5–10, New York, NY, USA, November 2016.

[2] Information Technology Laboratory Computer Security Division, "Zero trust architecture: comment on draft NIST SP 800-207 | CSRC," 2019, https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207.

[3] A. Chuvakin, "Named: endpoint threat detection & response," 2013, https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/.

[4] E. Mistek, M. A. Fikiet, S. R. Khandasammy, and I. K. Lednev, "Toward locard's exchange principle: recent developments in forensic trace evidence analysis," *Analytical Chemistry*, vol. 91, no. 1, pp. 637–654, 2019.

[5] J. Aguado-Delgado, J.-M. Gutiérrez-Martínez, J. R. Hilera, L.de. Marcos, and S. Otón, "Accessibility in video games: a systematic review," *University Access in the Information Society*, 2018.

[6] R. Armstrong, B. J. Hall, J. Doyle, and E. Waters, "Scoping the scope' of a cochrane review," *Journal of Public Health*, vol. 33, no. 1, pp. 147–150, 2011.

[7] BioCatch, "From Login to Logout: Continuous Authentication with Behavioral Biometrics," 2019, https://www.biocatch.com/resources/white-paper/from-login-to-logout-continuous-authentication-with-behavioral-biometrics.

[8] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia, Computer Science*, vol. 34, pp. 532–537, 2014.

[9] H. Arksey and L. O'Malley, "Scoping studies: towards a methodological framework," *International Journal of Social Research Methodology*, vol. 8, no. 1, pp. 19–32, 2005.

[10] I. López-Navarro, A. I. Moreno, M. A. Quintanilla, and J. Rey-Rocha, "Why do I publish research articles in English instead of my own language? differences in Spanish researchers' motivations across scientific domains," *Scientometrics*, vol. 103, no. 3, pp. 939–976, 2015.

[11] G. Ryu, S. Park, D. Choi et al., "Active authentication experiments using actual application usage log," in *Proceedings of the ASIA CCS'18: ACM Asia Conference on Computer and Communications Security Incheon, Incheon, Republic of Korea*, June 2018.

[12] P. Peris-Lopez, L. González-Manzano, C. Camara, and J. M. de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things," *Future Generation Computer Systems*, vol. 81, pp. 67–77, 2018.

[13] A. E. d. Oliveira, G. H. M. B. Motta, and L. V. Batista, "A multibiometric access control architecture for continuous authentication," in *Proceedings of the 2010 IEEE International Conference on Intelligence and Security Informatics*, p. 171, Vancover, Canada, May 2010.

[14] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: an experimental study on smartphones," in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, SOUPS '14*, pp. 187–198, USENIX Association, Menlo Park, CA, USA, July 2014.

[15] J. Wang, M. Ni, F. Wu, S. Liu, J. Qin, and R. Zhu, "Electromagnetic radiation based continuous authentication in edge computing enabled internet of things," *Journal of Systems Architecture*, vol. 96, pp. 53–61, 2019.

[16] J. Chauhan, H. J. Asghar, A. Mahanti, and M. A. Kaafar, "Gesture-based continuous authentication for wearable devices: the smart glasses use case," in *Applied Cryptography and Network Security, Lecture Notes in Computer Science*, M. Manulis, A.-R. Sadeghi, and S. Schneider, Eds., pp. 648–665, Springer International Publishing, New York, NY, USA, 2016.

[17] Z. Sitová, J. Sedenka, Q. Yang et al., "HMOG: new behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.

[18] I. Nakanishi and T. Yoshikawa, "Brain waves as unconscious biometrics towards continuous authentication-the effects of introducing PCA into feature extraction," in *Proceedings of the 2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS*, pp. 422–425, Nusa Dua Bali, Indonesia, November 2015.

[19] M. Shozawa, R. Yokote, S. Hidano, C.-H. Wu, and Y. Matsuyama, "Brain signal based continuous authentication: functional NIRS approach," in *Advances in Computational Intelligence*, I. Rojas, G. Joya, and J. Cabestany, Eds., pp. 171–180, Springer, New York, NY, USA, 2013.

[20] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: exposing insider threats using eye movement biometrics," *ACM Transactions on Privacy and Security*, vol. 19, no. 1, pp. 1–31, 2016.

[21] P. Tsai, M. K. Khan, J. Pan, and B. Liao, "Interactive artificial bee colony supported passive continuous authentication system," *IEEE Systems Journal*, vol. 8, no. 2, pp. 395–405, 2014.

[22] S. R. d. L. Silva Filho and M. Roisenberg, "Continuous authentication by keystroke dynamics using committee machines," in *Intelligence and Security Informatics, Lecture Notes in Computer Science*, S. Mehrotra, D. D. Zeng, H. Chen, B. Thuraisingham, and F.-Y. Wang, Eds., pp. 686-687, Springer, New York, NY, USA, 2011.

[23] E. C. Popovici, L. A. Stancu, O. G. Guta, S. C. Arseni, and O. Fratu, "Combined use of pattern recognition algorithms for keystroke-based continuous authentication system," in *Proceedings of the 2014 10th International Conference on Communications (COMM)*, pp. 1–4, Toronto, Canada, May 2014.

[24] U. Mahbub, J. Komulainen, D. Ferreira, and R. Chellappa, "Continuous Authentication of Smartphones Based on Application Usage," 2018, https://arxiv.org/abs/1808.03319.

[25] M. Smith-Creasey and M. Rajarajan, "A novel word-independent gesture-typing continuous authentication scheme for mobile devices," *Computers and Security*, vol. 83, pp. 140–150, 2019.

[26] A. Roy, T. Halevi, and N. Memon, "An HMM-based behavior modeling approach for continuous mobile authentication," in *Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3789–3793, Florence, Italy, May 2014.

[27] Ananya and S. Singh, "Keystroke dynamics for continuous authentication," in *Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pp. 205–208, Noida, India, January 2018.

[28] A. Acar and H. Aksu, A. Selcuk uluagac and K. akkaya, WACA: wearable-assisted continuous authentication," 2018, https://arxiv.org/abs/1802.10417.

[29] W. Commons, "Tinderbox eigenfaces models," 2019, https://en.wikipedia.org/w/index.php?title=File:Tinderbox_eigenfaces_models.jpg&oldid=887229639.

[30] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

2.3 Resumen de los resultados del artículo 1

En este capítulo se ha presentado un estudio sistemático de la literatura en el que se han contextualizado los diferentes enfoques que puede tener un sistema de autenticación continua, así como las pautas a la hora de evaluar su eficacia. Para ello se ha diseñado una metodología de búsqueda y cribado que, partiendo de 120 trabajos de investigación, todos ellos de medios con evaluación por pares, ha permitido seleccionar los 30 de mayor en el ámbito de la autenticación continua.

Se han extraído diferentes fuentes de datos, involucradas en diferentes ámbitos tecnológicos (e.g., teléfonos, ordenadores, etc.), y algoritmos de procesado. Pero dos de los avances más significativos, y especialmente relevantes para el posterior desarrollo de esta tesis, han sido la obtención de una síntesis de los criterios de categorización de sistemas de autenticación continua, en función de la permanencia y la singularidad; y la enumeración de las pautas para evaluar su eficacia en diferentes escenarios, estrechamente relacionados con la categorización anterior.

Los resultados evidencian que no está resuelto el mantenimiento de la identidad a largo plazo, aunque muestran una clara tendencia de las líneas de investigación hacia la implantación de la autenticación continua en tecnologías móviles. Sin embargo, es difícil abordar una tecnología tan cambiante, que además cuenta cada vez más restricciones de seguridad a la hora de utilizar funciones invasivas desde el punto de vista de la privacidad, como pueden ser todas aquellas relacionadas con la monitorización y la biometría conductual, necesarias para la autenticación continua.

Uno de los mecanismos con mayor recorrido es el del estudio de las métricas de tecleo, tanto en el ámbito de los ordenadores como el de los teléfonos móviles, con sutiles diferencias a la hora de procesar los datos biométricos, debidas principalmente al cambio de un teclado físico a uno virtual. Existen en la literatura numerosas investigaciones centradas en el área de la autenticación continua mediante teclados virtuales, pero los resultados de dichas investigaciones no pueden ser comparados directamente, bien por arrojar distintas métricas, por seguir diferentes metodologías, o incluso por evaluar las mismas características, pero utilizando diferentes datos de entrada (e.g., se puede medir el movimiento de la mano a través de los gestos sobre la pantalla, del acelerómetro del dispositivo, etc.). En el siguiente capítulo se abordará un profundo análisis de esta tecnología.

Capítulo 3

Autenticación dinámica mediante el uso de secretos precompartidos

3.1 Contribución del artículo 2

Los sistemas de *port-knocking* aportan una capa adicional de seguridad en las conexiones con servicios remotos, ocultando tras un *firewall* el servicio a proteger hasta que el usuario no haya "golpeado" (i.e., interactuado mediante algún tipo de conexión) una serie de puertos en un orden predeterminado. Por lo tanto es un sistema de autorización basado en una secuencia secreta precompartida de puertos, que ofrece una solución sencilla ante adversarios que busquen autenticarse mediante fuerza bruta, o dispongan de algún tipo de ataque *zero-day*, porque no podrán interactuar con el servicio si no conocen esta combinación.

Sin embargo, cuando se realiza este golpeo de puertos, si el adversario en cuestión tiene acceso al contenido de las conexiones, esta secuencia queda expuesta y el sistema se vuelve completamente ineficaz. Este puede ser el caso al que se enfrente dispositivos instalados en una red local que, aun estando en un segmento relativamente confiable, deban tener una interfaz de administración, y se desee que esta esté protegida; como es el caso de los dispositivos IoT presentes en entornos hospitalarios.

El problema al que se enfrenta el *port-knocking* ante este tipo de adversarios, aunque parte del ámbito de los sistemas de autorización (i.e., no valida una identidad, sino que otorga o deniega permisos de acceso), guarda una estrecha relación con el problema que afronta la autenticación continua: desarrollar sistemas dinámicos y resilientes ante suplantaciones que, en este caso, se materializarían como ataques de repetición.

Utilizando un sistema dinámico basado en tokens que, procesados, generen periódicamente un valor que permita al autenticador validar el acceso a los sistemas protegidos, se podrá abordar esta problemática. Cualquier medida de seguridad que se introduzca debe contar, también, con una evaluación del impacto que tiene para la usabilidad; por

lo que este sistema debe tratar de descansar, en la medida de lo posible, sobre sistemas conocidos y aceptados por los usuarios.

Este capítulo, a través del artículo presentado, se expone una propuesta que permite abordar dicho problema utilizando los principios de la autenticación continua. Mediante el uso de un secreto precompartido que servirá como semilla de un generador de números pseudoaleatorio, en lugar de como una secuencia de golpeo, se establecerá cada 30 segundos una nueva lista puertos a través de un sistema TOTP similar al utilizado como segundo factor de autenticación en la mayoría de las plataformas online. De esta forma se garantiza que el usuario legítimo tenga sincronía con el sistema a proteger, y que un adversario que, eventualmente, tuviese conocimiento de la secuencia de golpeo, no pudiese explotarla más que durante una pequeña ventana de tiempo.

3.2 Artículo 2

A continuación se presenta el artículo 2 del compendio, "*C-Lock: Local Network Resilient Port Knocking System Based on TOTP*" publicado en la revista *Wireless Communications and Mobile Computing*, de la editorial Wiley-Hindawi.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9153868, 9 pages
https://doi.org/10.1155/2022/9153868

Research Article

C-Lock: Local Network Resilient Port Knocking System Based on TOTP

Javier Junquera-Sánchez, Carlos Cilleruelo, Luis de-Marcos, and José-Javier Martinez-Herráiz

Department of Computer Science, Universidad de Alcalá, Spain

Correspondence should be addressed to Carlos Cilleruelo; carlos.cilleruelo@uah.es

Received 3 June 2021; Revised 20 October 2021; Accepted 26 November 2021; Published 31 January 2022

Academic Editor: Dapeng Wu

Port knocking is an access-control technique that consists of revealing a network protected resource only to those users that can prove they know a preshared port sequence. This proving process is done by connecting to the defined ports in the correct order; so, the list gets exposed to the adversaries with access to the connection's channel. We propose a newfangled technique for protecting this process, avoiding eavesdroppers to get a long-live valid sequence. Our method is based on TOTP codes and has been designed thinking on making it the most usable as possible. There has been designed two different approaches, but we demonstrate that the most simple of them is far enough robust, while it remains to be very usable. This technique is especially suitable for enhancing the resilience of network services against local network adversaries.

1. Introduction

In a worldwide connected network, where almost all servers have to be remotely administrated, access control has become a crucial task in data protection. As Telnet was in the past, nowadays, the most popular protocol for remote administration is SSH (Secure Shell) [1]. The hardening of SSH service has been widely addressed by the security experts, concluding that network segmentation (such as VPN or VLAN) and packet filtering in earlier network stages could be the most effective approaches for it. However, there are scenarios where this kind of measures are not feasible or are completely ineffective.

One of the most utilized security measures for hardening SSH services is port knocking. Port knocking is an inexpensive protection technique that consists of denying the connection to a targeted port until a preshared set of ports has not been "knocked" (i.e. contacted somehow) in a certain order (i.e., until these ports have not received a connection from the client, the protected port will not be opened).

Some approaches could seem similar, like changing the default port for other (e.g., change the SSH's port from 22 to 2222), but they are just "security through obscurity" measures that could be useful to avoid some automatic attacks, but ineffective against a simple network scan [2]. By contrast, port knocking is generally accepted to be effective both as a second authentication factor and filtering technique [3].

Even so, against certain adversaries, port knocking lacks effectiveness, and it becomes necessary to find alternatives and improvements. These adversaries are mainly

(1) Adversaries with enough time for finding the correct knock sequence

(2) Adversaries with eavesdropping capabilities

This is the case of some IoT (Internet of things) devices that may not have enough capabilities for creating an isolated network (just for themselves). But if they can filter incoming connections, then it can detect a port knocking sequence. In particular, it can be applied to medical environments where it is necessary to install network-connected medical devices, whose configuration cannot be modified (or cannot even be known) at the risk of loss of guarantee, and whose security is not reliable. As Ben-Gurion researches

showed [4], there is an increasing myriad of unpatched medical devices connected to medical networks which could be easily used for pivoting through network segments.

IoT devices can be mainly categorized into two types [5]: devices with high resources (e.g., Raspberry PI-based) or with low resources (e.g., based on Arduino or other microcontrollers). Often, as IoT devices that are implemented in low resource hardware, developers have to optimize their power consumption, and they are deployed without implementing any security control [6]. This leverages to a high-risk scenario for information security, where the most common threaths are signal jamming attacks and replay attacks [6]. Signal jamming consists of that the adversary interferes with communication between two systems. This interference can be done via several technologies, like RFID (radio-frequency identification). But as IoT is widely implemented also using common mobile technologies (e.g., Android, and Raspberry PI), both attacks (i.e., signal jamming and replay attacks) can be performed using well-known techniques.

These well-known techniques are often inherited from traditional computer networks attacks. Some of them are mitigated simply by correlating data about the genuine devices to detect and evade intruders [7], because some IoT devices require low-cost specifications. But as the complexity of the system grows (even though it means the attack surface also grows), advance defense techniques can be implemented.

The present work is aimed at providing a mitigation to the risks that port knocking faces against local network adversaries (whose origin is mainly placed on replay attacks) and provides the design of a soundness port knocking model which also brings resilience against local network-related attacks. Even though the findings of this paper have been detected having in mind medical environments, our proposal is valid for many other scenarios (especially, any scenario where a local adversary could be present).

We have also put our efforts in designing the model following industry standards, based on the most usable and secure techniques, to increase the likelihood of its successful implementation in real environments.

The remainder of this document follows the next structure: In Section II, we study the different elements that compound our scheme and its context. In Section III, we analyze the different adversaries that a port knocking system could face. In Section IV and Section V, we describe our system and analyze its properties. Finally, in Section VI, we extract the conclusions of our analysis.

2. Background

2.1. Port Knocking. The most basic port knocking system, proposed in [8], consists in establishing a secret set of ports that must be interacted with before a protected port gets revealed. Figure 1 shows the process for establishing an SSH connection, with the ports 1234, 5678, and 9012 defined as the secret set.

One of the most popular implementations (in fact, the official Debian's port knocking package [9]) was developed

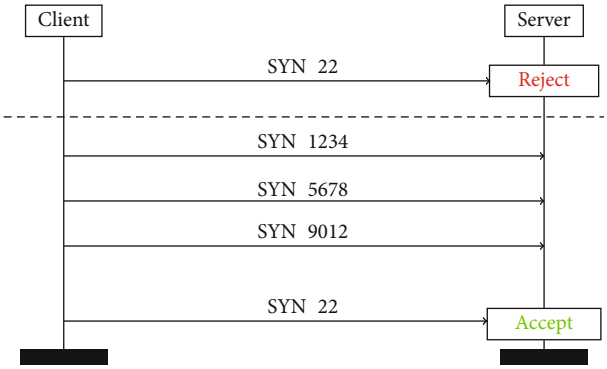

Figure 1: Port knocking process.

by Judd Vinet [10], but there are many references about how to implement this security technique. One very well documented could be read in [11].

The objective of port knocking is not just putting a facade to service for avoiding configure it correctly (which is highly discouraged). Even a correctly secured service could be the victim of a zero-day attack [12], and ensuring that only a certain number of clients can interact with it, and could be the only effective action against it.

It is necessary to understand that port knocking is not a system per se, but an authentication procedure. And consequently has to be analyzed as an authentication procedure, caring about all the issues these systems could face [13].

By contrast, the single package authentication approach [14] relies on a mechanism where the client, to be allowed to connect, has to prove his by identity sending a special package to the server.

2.2. TOTP. Another core element of our proposal is TOTP. TOTP is a HOTP-based algorithm (HMAC-based one-time password) [15] for generating time-based OTP codes. Using TOTP, two sides of communication can mutually authenticate themselves with a high-security degree, just using simple and ephemeral numeric codes.

HOTP codes are generated, broadly, applying an HMAC function [16] to a counter code. This counter (also known as moving factor) acts as a kind of ratchet [17] and usually means the time a security event has happened for ensuring mutual authentication (e.g., the times a remote controller has been used, for opening a car). In TOTP, the code is defined as the 30 second slots "elapsed since midnight UTC of January 1, 1970" [18].

TOTP is a de facto standard for providing two-factor authentication and is widely implemented as an online account access control approach (like Google, Facebook, and many others do). To prove his identity, after entering his password, a user has to provide a numeric code generated by an application or a smart-card where they have previously installed a special code.

This process is simply a TOTP code generation, based on a shared secret (usually codified in the QR code) and is used for authenticating that the user who provides the login password is the same person that was registered at the sign-up stage.

It can also be applicated in the prevention of replay attacks [19], and even though it should be sent over secure channels (i.e., encrypted like IPSec or SSL [20], the key must be strong enough for resisting unprotected transmissions without putting the generation system on risk.

2.3. Related Work. There have been several researches focused on improving port knocking systems. In [21], the authors analyze what they call NAT-knocking problem, which happens when both the legit client and the attacker are behind the same NAT. In this case, the attacker could impersonate the client because, after the knocking process, the server just identifies the genuine client by his IP address. In addition, they refer to problems related to the overload that port knocking could cause to the server (DOS-Knocking attack), but this issue had been previously addressed using 2FA [22].

Moreover, sending multiple factors for hardening the port knocking authentication process has been widely studied by [23]. They also detect the difficulty of associating the identity of the client who authenticates (who does the knocking process) with who connects (the one who later establishes the connection with the protected port).

Finally, the time synchronization between client and server has been proposed as a way of randomizing the knocking sequence. In [24], they use the time as part of the seed for an RNG, which determines the knock sequence every time it receives a connection.

2.4. Adversary Modeling. The port knocking's authentication process is more similar to a monologue than to a conversation. This fact is very relevant both for defining our adversary model and for the later analysis.

From now on, we will have to present those four actors:

(i) Protected service: the service that must not be exposed to anyone who does not know the correct knock sequence

(ii) Server: the host where the protected service is located. It will also be the oracle for checking the port combination

(iii) Client: the genuine user who knows the shared secret necessary for solving the port knocking sequence and accessing the protected service

(iv) Adversaries: those actors (semihonest or malicious) who should never access the protected service

Unless otherwise indicated, when we talk about authentication, we are referring to the port knocking process (i.e., not the secret service or other authentication processes).

2.5. Assumptions. The server will always be online and accessible at least to every user in a local network.

(i) The cryptographic elements implemented (i.e., cypher suites and TOTP) are robust

(ii) The firewall system is secure

(iii) There exists a preshared secret between the client and the server, has been generated with a secure PRNG, and has been securely shared

(iv) The protected service has its security measures correctly implemented (i.e., secure authentication and attack detection)

Concerning our model, it must comply with the following specifications:

(i) After a correct knocking sequence, the protected service will only be available for a short period for new connections, and only from the same source

(ii) Firewall will allow established connections (i.e., if after the port knocking, a correct authentication against the protected service is done, and this connection must not be denied after the time)

2.6. Adversary Goals. As the adversary never should know how to solve the protected service's security challenges (e.g., the SSH credentials), his goal should be to be able to access the protected service anywhere he wants (e.g., for brute forcing).

This can be done well by acquiring the capability to generate the knocking sequence anytime (e.g., retrieving the secret key) or forcing the client to repeat it arbitrarily.

2.7. Capabilities. In the worst case, our adversary will be a Dolev–Yao's adversary [25], which, in practice, means that the only limit to his capabilities is those related to the cryptographic techniques used.

(i) Knows the algorithm

(ii) Runs in polynomial time

(iii) Can interact anytime with the server and with the network (i.e., has eavesdropping and tampering capabilities)

(iv) Does not know the preshared secret

Depending on his attitude, we could distinguish three possible adversaries:

(1) Honest-but-curious: an eavesdropper who can retrieve the knock sequence played by the client

(2) Malicious online (active in authentication time): can tamper the connection during the knock sequence or even impersonate the client's IP

(3) Malicious online (active after port knocking time): can force the client to replay the knock sequence (e.g., interrupting an established connection, so the client has to connect again)

Malicious offline adversaries are not taken into account because, as argued in security, they would not suppose a threat.

2.8. Proposed Model. Without ever ignoring security, usability is a fundamental pillar of this model, as its effectiveness and its acceptance depend on it [26]. These objectives will be achieved following security guidelines and using industry state of art technologies. Aditionally, user-side functionality has been designed; so, the user will not need anything else than well-known tools (i.e., would not need to install new software to use the solution).

2.9. Setup. To guarantee the correct construction of the TOTP codes, both client and server have to be time synchronized. The best way is using an NTP server, but this functionality has to be provided by third parties (i.e., a public time server) to fulfill our compatibility principle (e.g., the user has to be able to configure its TOTP generator using Google Authenticator) [27].

After the server administrator configures which service should be protected (as in a regular port knocking system), the shared secret is established in the server. This secret must be generated using a secure PRNG [28] and must be at least 160 bits long. According to TOTP's RFC requirements: "The keys MAY be stored in a tamper-resistant device and SHOULD be protected against unauthorized access and usage" [18].

On the client's side, the shared secret will not necessarily be stored in the device that will do the authentication (the client itself). In fact, in most cases, it will be into the device of an operator (e.g., its mobile phone), who will just introduce the TOTP code in the client when the authentication is required.

The sharing method must be human-friendly and easy to read by an external device. The proposed procedure for achieving this purpose is using both a base 32 representation and a QR code. This method (illustrated in Figure 2) is the most common way of setting up 2FA in web services.

After the previous step, the system is ready. The protected service is hidden behind the firewall, and the server starts to wait for the first port knocking sequence.

2.10. Port Sequence Generation. The first time slot's lifetime will lasts the time gap between the epoch timestamp $t0$ [29] and the next timestamp t such that $t \equiv 0 \pmod{30}$. After that moment, a new port set is generated each 30 seconds.

Figure 1 shows the algorithm designed for the port generation. The initialization process is very simple, just consists in generating the TOTP code. The substantial part of the algorithm construction has been how to generate the port set with this code. And here is where we have found the most serious conflict between usability and security.

The main benefit of this strategy is that the number of ports for the knocking could be increased (to increase the knocking effort) without increasing the generation cost (as it stills depending on the same seed), but requires special software in the client's side for processing the TOTP.

On the other hand, the second strategy just requires the TOTP code for generating the knocking sequence. Each port would be mapped to a pair of digits from the TOTP code and added to a mask. The proposed mask has not been arbitrarily chosen, but $0 \times C000$ (49152) marks the start of the dynamic ports range [30], and $0 \times C030$ is the first number that ends with two zeros. These ports have been selected due to the following:

Figure 2: Sharing secret.

(1) No service should be listening on them (this way, we avoid disruptions)

(2) In consequence, it is very difficult to receive a SYN request (i.e., something that could be interpreted as a knock)

(3) Using $0 \times C030$ instead of $0 \times C000$ allows the user to replace the two trailing zeros with the TOTP's corresponding value, instead of having to calculate the sum

With this alternative strategy, no additional software would be needed in the client. The knock sequence could be easily derived by a human from the TOTP code, and it could even be reproduced using a web browser.

2.11. Authentication Process. Once calculated the knock sequence, the client haves to reproduce it. The server will interpret every SYN message as a knock; so, the client has to follow the algorithm, connecting in the correct order to each sequence's port.

We have selected SYN to characterize a knock for compatibility because almost any software with network capabilities will be able to generate it (as commented previously, in the worst case, it could be reproduced with a web browser).

A complete TCP handshake has been discarded as it would require an active service for the interaction (what could suppose overload). Also, it is easier to allow (as far as secure firewall configuration is concerned) the port knocking service to listen to SYN messages, than allowing complete input connections (especially in those port ranges).

After a first correct knock from an IP address, the server saves an internal state for this source (as shown in Figure 3). If the next knock is also correct (following the sequence), the state is changed, otherwise, is deleted. When a user has correctly reproduced the complete sequence, the server adds a rule in the firewall for letting him connect to the protected service for 30 seconds.

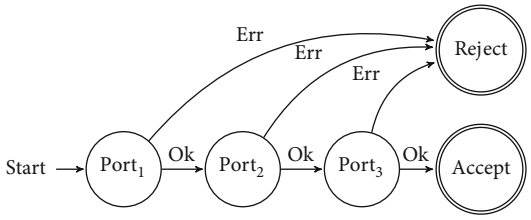

Figure 3: Sequence evaluation.

2.12. Example Scenario. Due to the versatility and functionality of c-lock, this system can be applied to multiple network architectures and scenarios. One example scenario will be to apply c-lock in a health environment, like a hospital.

As a critical system, hospitals are in great need of cybersecurity [31]. Also, hospitals need to bring security to medical devices, and they cannot or modify these medical devices. This situation generates a problem, how to offer security to devices that you cannot modify or operate [32]?

One possible solution to this problem is to involve firewalls in order to access and communicate with these devices. In the designing and implementation process of a network architecture, we can involve the use of firewalls in front of all medical devices. There are numerous firewalls, open source, and not that are Linux-based, and c-lock could be easily deployed in them.

Furthermore, we will be involving 2FA without affecting their daily use or default installation. However, it is implicit that good network segmentation is crucial for the security of this system. Firewalls running c-lock should be the only way of communication with these devices.

3. Discussion

The proposed method was designed for systems with packet filter capacities (i.e., in contrast with those IoT systems with low complexity-cost specifications, like integrated circuits). As the main purpose of the method is to protect access to administration interfaces (e.g., SSH), it should not exceed any computational constraint.

Implementing this method is also costly free in computational terms for this type of system, i.e., should not imply any overhead in contrast with a classical port-knocking process, as it should also be executed once per SSH session, and it is based on trivial operations. However, it would be necessary to modify the operational procedures to add the port knocking step before starting the administration sessions.

3.1. Security. The model has been analyzed under the principles discussed in [33]. We have chosen an unbounded scenario, where an infinite number of sessions could be played by the adversary.

As previously told (see section Adversary modeling), the analysis of a port knocking system has some peculiarities. In particular, using a symbolic approach in a model where there is just one player sending messages may not show relevant results [34]. Given that, and even though we have picked elements from other verification schemes, the strength of the system will be measured using a cryptographic approach.

Assuming that TOTP generation is secure, the simplest way for an adversary to determine the key which (would let him generate correct port sequences) will be the exhaustive search [35]. This approach, according to [36], would take more than 10 years for our key size and algorithms. So then, it should not exist a successful offline attacker.

We have evaluated our model as a computational complexity problem where the average effort for breaking it and should take more than 30 seconds (the time slot's length) to be carried out. This analysis has also led us to determine if is secure to implement the most usable port generation strategy (strategy B showed in Algorithm 1).

There are $1e6$ different combinations in both strategies. It is trivial to check this fact in approach B, where the port numbers are directly extracted from the TOTP code (and it has 6 digits). Approach A combinations depend on HOTP. HOTP is a deterministic function which, in the space of the TOTP code, and for more than 2 different moving factors, makes the port generation function injective (i.e., the probability that 2 different TOTP codes generate the same set with three or more ports is negligible) (see Lemma 1)). So then, strategy A generates also $1e6$ different combinations.

Lemma 1. (Strategy A is injective). *HOTP:* $\mathbb{R} \times \mathbb{Z} \longrightarrow \mathbb{Z}1e6$

$$\begin{aligned} F : \mathbb{Z} \times \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{B}/F(x, y, z) \Leftrightarrow \boldsymbol{hotp}(x, y) = \boldsymbol{hotp}(x, z), \\ \forall a, b \in \mathbb{Z}_{1e6} | a \neq b | \forall x &\Rightarrow Qx = P(F(x, a, b)) = 1/1e6, \\ \forall y | y > 2 &\Rightarrow Q_0 Q_1 \cdots Q_y = (1/1e6)^y \sim 0. \end{aligned} \tag{1}$$

Therefore, the adversary's effort will depend on how each strategy should be executed.

3.2. Adversary Effort. We have to define some variables to calculate the effort that an adversary should do to succeed and how much time would it cost. Each round (i.e., each complete knocking sequence followed by checking the status of the protected port) runs over these parameters:

(i) The time for computing the HOTP code is negligible because it could even be precomputed

(ii) Each port sequence has n ports, and each port is codified with two digits of the TOTP code. So, there would exist $1e(2n) = 10^{2n}$ possible codes

(iii) The time for executing each knock lasts K time (with K semiconstant, defined by the time for sending a SYN message)

(iv) After the last correct knock, the protected service gets exposed after y time

Consequently, for both strategies, each round will last $n \cdot K + y$ seconds. In strategy A, n and y could be configured in the implementation, while in strategy B, just y can be set. As a result of that, the effort for testing all

Initialization
1: $tSlot \leftarrow epochT\ imestamp()//30$ {//means integer division}
2: $totp \leftarrow hotp(tSlot, sk)$ {*e.g.*123456}
Strategy A
1: **for** $n \leftarrow 0$ **to** 3 **do**
2:**begin**
3:$aux \leftarrow hotp(n, totp)$
4:$port[n] \leftarrow (aux\%65534) + 1$ {$0 < port < 65535$}
5:**end**
Strategy B
1: $mask \leftarrow$ 0xC030 {0xC030 = 49200}
2:$p_{aux}[0] \leftarrow (totp//1e4)$ {*e.g.*12}
3:$p_{aux}[1] \leftarrow (totp//1e2) - (p_{aux}[0] * 1e2)$ {*e.g.*34}
4:$p_{aux}[2] \leftarrow (totp) - (p_{aux}[1] * 1e2) - (p_{aux}[0] * 1e4)$ {*e.g.*56}
5: **for** $n \leftarrow 0$ **to** 3 **do**
6:**begin**
7:$port[n] \leftarrow mask + paux[n]$ {$port[0]$ = 0xC030+12 = 49212}
8:**end**

Algorithm 1: Port generation algorithm.

combinations would be $10^{2n} \cdot (K + y)$, and the average effort for finding a successful random port set will be $10e(2n) \cdot (K + y)$ seconds.

With an equal fixed port set length (e.g., 3 ports in the two strategies), the requirement for an adversary to not be able to break the system (i.e., not generating a correct sequence in less than 30 seconds) is that $y > (30^2 - 10^6 \cdot K)/10^6$.

In the practice, this means that in a highly unlikely scenario where a SYN message is sent instantly, y should be greater than $9e$ (−3). Moreover, when the adversary would find a correct sequence (i.e., after almost spent 16 hours, setting y to one second), he would only be able to attack the protected service during less than 30 seconds.

And all that without regarding the noise it would make.

3.3. Other Attacks. As it is a passive system (like the previous works), it is not vulnerable to port scans (it just listens and modifies its internal states), depending on his attitude.

The only profit an honest-but-curious adversary could take is eavesdropping the knock sequence and makes a replay attack. Repeating the sequence (as long as it is done in the same timeslot) would let him access to the protected service, but only during 30 seconds. The legit client just sends the knock sequence once, and its connection to the protected service stays for a while; so, this adversary will have few chances of success.

From a malicious adversary perspective, there could be two different types of attacks related to achieving his goals. The malicious adversary could be active during the authentication process or after it.

During the authentication process, an adversary could tamper the communication through a man-in-the-middle attack, so that he could use the client as a code generator. It would work as follows:

(1) The adversary kills the established connection, to force the client to authenticate again

(2) The client sends the port sequence, and the adversary uses it to authenticate himself

(3) When the client tries to reach the protected service, the adversary answers with a fake rejection

(4) Then the client, believing there could have been an error, would send again the sequence or wait until the next timeslot to repeat the process

If the TOTP code was generated by the client (instead of introduced by an operator), and the authentication was done by an automatical process, the adversary could be able to repeat this process indefinitely. With an operator-controlled authentication, this attack would be easier to detect, because after some failures the operator would notice that something is happening.

The other active attack (after the authentication process) would be similar to the passive approach. Instead of replaying the sequence, after successful authentication, the adversary could impersonate the client's IP address for accessing the protected service. This approach would only let him access to the protected service for 30 seconds unless he launches other attacks (oriented to exploit the protected service, not the port knocking authentication).

In none of these attacks, the adversary would be able to forge correct port sequences.

3.4. Contribution. In contrast with the classic port knocking model, which could be defeated after just one client's authentication (i.e., an eavesdropper just needs to listen one connection to retrieve the knocking sequence), our model is not vulnerable to eavesdropping. If an adversary obtains a correct set of ports, it will only be able to use it in the remaining time until the next timeslot (i.e. less than 30 seconds).

In our scenario, the NAT knocking attack [21] would not be feasible, because all participants would be in the same network segment. The server just calculates the knocking

Table 1: Time complexity vs. adversary effort.

n	Sequence calculation (s)	Avg. adv. effort (s)	Avg. adv. effort [$y = 1$ s] (s)
1	3.0000e −04	0.22	10.00
2	2.0503e −05	2.23	100.01
3	1.8358e-05	22.36	1000.12
4	2.0980e −05	223.60	10001.24
5	2.4557e −05	2236.06	100012.49
6	2.7894e −05	22360.67	1000124.99
7	3.1232e −05	223606.79	10001249.92
8	3.4809e −05	2236067.97	100012499.21
9	3.8385e −05	22360679.77	1000124992.18

sequence once at the start of the timeslot; so, DOS-knocking attack [21] would also be useless.

Our approach avoids the overload that [24] could generate in the system. The complexity of our model, with a fixed knock sequence length, is O (1) for computing the knock sequence, and if it is computed every time the time-slot changes (i.e., instead of when the client tries to connect), it would not cause any significant overhead. Table 1 shows a server-side time analysis for calculating n ports and the average effort (in seconds) it would suppose for an adversary guess in the sequence with just a latency of 0.25 ms (i.e., the minimum latency required for critical IoT applications [37]), and with the y value set in one second (as discussed in the Adversary Effort subsection).

Besides, our model (in special, configured with the strategy B) is more versatile when being used by different types of clients and systems. Thirdly, generating the port sequence using TOTP, instead of a custom method, is more secure and verifiable ([38].

4. Conclusions

The model proposed provides the necessary elements to introduce port knocking systems in local networks in a secure manner. With our system, an adversary will not be able to take profit from an eavesdropped authentication process. Moreover, he would not be able to craft a correct port knocking sequence.

Therefore, we have achieved our goals: the model is secure, efficient, and very usable. Even though the port generation could be more complex (as occurs with port generation strategy A), we have proven that it will not increase significantly the security. Additionally, it would involve unnecessary complexity in the client, while with a simple method (i.e., port generation strategy B), we can assemble a long-lived security system.

The system should be constructed using strategy B. Furthermore, if strengthen the system's resilience was required (something that because of the results might not happen), it would be enough with incrementing the time between the last correct knock and protected service opening.

4.1. Future Work. An adversary could take advantage of an incorrect implementation. If it is necessary, an automatically triggered authentication should be limited to the number of retries after an error. If the retries number overcomes a threshold, supervision should be required.

All the elements out of our system scope should be configured following the best practices of security. Finally, the model has been designed to be used for just one client (more specifically, with just one preshared key).

It would be great to verify the system using automatical protocol provers (e.g., Tamarin Prover ([39]; [40]), addressing also the secret key sharing process and the introduction of the TOTP code in the client.

Nevertheless, the most attractive research path could be its extension for a multiclient scenario. As the TOTP standard foresees the generation of up 10 digits codes, it could be studied its usage. Studying if TOTP-based port switching could be implemented in a SPA approach might also yield interesting results.

Data Availability

Data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 Research and Innovation Program under grant agreement No. 826284 (ProTego).

References

[1] J. Geerling, *Ansible for DevOps: Server and Configuration Management for Humans [Google-Books-ID: oLuVjgEACAAJ]*, 2015, LeanPub.

[2] D. Stuttard, "Security & obscurity," *Network Security*, vol. 2005, no. 7, pp. 10–12, 2005.

[3] S. Jeanquier, *An analysis of port knocking and single packet authorization, [M.S. thesis]*, Information Security Group Royal Holloway College, University of London, 2006.

[4] T. Mahler, N. Nissim, E. Shalom et al., "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," in *Presented at the RSNA Conference*, vol. 6, Chicago, IL, United States, 2017.

[5] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[6] F. Chantzis, I. Stais, P. Calderon, E. Deirmentzoglou, and B. Woods, *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*, No Starch Press, Inc, San Francisco, 2021.

[7] E. E. Tsiropoulou, J. S. Baras, S. Papavassiliou, and G. Qu, "On the mitigation of interference imposed by intruders in passive RFID networks," in *Decision and Game Theory for Security*, Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, and W. Casey, Eds., Springer International Publishing, Cham, 2016.

[8] M. Krzywinski, "Port knocking: network authentication across closed ports," *SysAdmin Magazine*, vol. 12, pp. 12–17, 2003.

[9] "Debian – el sistema operativo universal," 2020, https://www.debian.org/index.es.html.

[10] J. Vinet, "Knockd - a port-knocking server," 2020, https://zeroflux.org/projects/knock/.

[11] M. Doyle, *Implementing a Port Knocking System in c (Honors Thesis)*, The University of Arkansas, 2011.

[12] M. Rash, *Linux firewal ls*, No Starch Press, 2007, https://nostarch.com/firewalls.htm.

[13] M. Zviran and Z. Erlich, "Identification and authentication: technology and Implementation issues," *Communications of the Association for Information Systems*, vol. 17, no. 1, 2006.

[14] M. Rash, "Protecting SSH servers with single packet authorization," *Linux Journal*, vol. 2007, no. 157, p. 6, 2007.

[15] F. Hoornaert, D. Naccache, M. Bellare, and O. Ranen, "HOTP: An HMAC-based one- time password algorithm," (RFC No. 4226) [Library Catalog: https://tools.ietf.org]. 2020, https://tools.ietf.org/html/rfc4226.

[16] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: keyed-hashing for message authen- tication (RFC No. 2104)," 2020, https://tools.ietf.org/html/rfc2104.

[17] M. Bellare, A. C. Singh, J. Jaeger, M. Nyayapati, and I. Stepanovs, "Ratcheted encryption and key exchange: The security of messaging," in *Advances in cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds., Springer International Publishing, Cham, 2017.

[18] J. Rydell, M. Pei, and S. Machani, "TOTP: time-based one-time password algorithm (RFC no. 6238)," 2020, https://tools.ietf.org/html/rfc6238.

[19] A. S. M. Abukeshipa and T. S. M. Barhoom, *Implementation and Comparison of OTP Techniques (TOTP, HOTP, CROTP) to Prevent Replay Attack in RADIUS Protocol, [M.S. thesis]*, Islamic University of Gaza, 2014.

[20] M. L. T. Uymatiao and W. E. S. Yu, "Time-based OTP authentication via secure tunnel (TOAST): a mobile TOTP scheme using TLS seed exchange and encrypted offline keystore," in *2014 4th IEEE International Conference on Information Science and Technology*, Shenzhen, China, 2014.

[21] A. I. Manzanares, J. T. Márquez, J. M. Estevez-Tapiador, and J. C. H. Castro, "Attacks on port knocking authentication mechanism," in *Computational science and its applications – ICCSA 2005*, O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganá, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, Eds., Springer, Berlin, Heidelberg, 2005.

[22] D. Worth, *CÖK - cryptographic one-time knocking*, BlackHat, 2004, Retrieved May 2, 2020, from https://blackhat.com/presentations/bh-usa-04/bh-us-04-worth-up.pdf.

[23] R. de Graaf, J. Aycock, and M. Jacobson, "Improved port knocking with strong authentication," in *21st Annual Computer Security Applications Conference (ACSAC'05)*, Tucson, AZ, USA, 2005.

[24] T. Popeea, V. Olteanu, L. Gheorghe, and R. Rughiniș, "Extension of a port knocking client-server architecture with NTP synchronization," in *2011 RoEduNet International Conference 10th Edition: Networking in Education and Research*, Iasi, Romania, 2011.

[25] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[26] C. Braz and J.-M. Robert, "Security and Usability: The Case of the User Au- Thentication Methods," in *Proceedings of the 18th conference on l'interaction homme- machine*, Montreal, Canada, 2006.

[27] "Google Authenticator," 2020, https://play.google.com/store/apps/details?id=com.

[28] J. I. Schiller and S. Crocker, "Randomness requirements for security (RFC no. 4086)," 2020, https://tools.ietf.org/html/rfc4086.

[29] "Epoch (computing) [Page Version ID: 950077310]. (2020, April 10). In Wikipedia. Page Ver- sion ID: 950077310," 2020, https://en.wikipedia.org/w/index.php?title=Epoch_(computing)&oldid=950077310.

[30] J. Touch, "Recommendations on using assigned transport port numbers (RFC no. 7605)," 2020, https://tools.ietf.org/html/rfc7605.

[31] L. Coventry and D. Branley, "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[32] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices*, vol. 8, p. 305, 2015.

[33] S. Matsuo, K. Miyazaki, A. Otsuka, and D. Basin, "How to evaluate the security of real-life cryptographic protocols?," in *Financial Cryptography and Data Security*, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, and F. Sebé, Eds., Springer, Berlin, Heidelberg, 2010.

[34] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in crypto- logy — EUROCRYPT 2000*, B. Preneel, Ed., Springer, Berlin, Heidelberg, 2000.

[35] M. J. Wiener, "Exhaustive key search," in *Encyclopedia of Cryptography and Security*, H. C. A. Tilborg, Ed., Springer US, Boston, MA, 2005.

[36] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," in *Public Key Cryptography*, H. Imai, Y. Zheng, H. Imai, and Y. Zheng, Eds., Springer, Berlin, Heidelberg, 2000.

[37] P. Schulz, M. Matthe, H. Klessig et al., "Latency critical IoT applications in 5g: perspective on the design of radio interface and network architecture," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 70–78, 2017.

[38] W. M. S. Alves, T. L. Prado, A. M. Batista, and F. A. S. Ferrari, "The dangerous path towards your own cryptography method," 2018, https://arxiv.org/abs/1812.05440.

[39] B. Schmidt, *Formal analysis of key exchange protocols and physical protocols [Ph.D. thesis]*, ETH Zurich, 2012.

[40] "Tamarin prover," 2020, https://tamarin-prover.github.io.

3.3 Resumen de los resultados del artículo 2

Se ha expuesto una propuesta de modelo para introducir, de forma segura, sistemas de *port-knocking* en entornos donde los adversarios tengan capacidad de escucha de las comunicaciones. La propuesta aborda, mediante un sistema dinámico basado en códigos TOTP, el problema de autenticarse a través de un canal inseguro, permitiendo acotar y minimizar la ventana de tiempo en la que un adversario podría explotar una combinación de puertos, de haberle sido revelada. Se ha probado la seguridad del modelo evaluando la complejidad computacional que supondría evadirlo, bajo la perspectiva de diferentes adversarios; consiguiendo no sobrecargar el sistema a proteger, ni mermar, para el usuario legítimo, la usabilidad del sistema de *port-knocking*.

Una vez validada la comunicación entre el terminal (i.e., equipo cliente) y el servidor, queda pendiente la autenticación del operador que trabaja sobre dicho terminal. Aun siendo el modelo propuesto un sistema efectivo para gestionar la autorización de conexiones, sigue sin cubrir la validación de identidades individuales, con la consecuente amenaza de una eventual suplantación del usuario que opera el dispositivo en el que se almacenan las claves precompartidas. Para abordarlo desde una perspectiva de seguridad adaptativa, realizaremos un estudio del estado del arte de los sistemas de autenticación continua.

Capítulo 4

Estudio de sistemas de autenticación continua basados en biometría conductual

4.1 Contribución del artículo 3

Pese a ser una de las aproximaciones más populares en la literatura, la diversidad de metodologías y técnicas de evaluación que tratan los patrones de tecleo como un elemento biométrico complica su análisis a la hora de desarrollar un sistema de autenticación continua implantable en el control de accesos. Además, la extrapolación de los resultados clásicos al ámbito de los teclados virtuales (i.e., los utilizados por los dispositivos móviles) no es trivial, y se acompaña habitualmente de datos de otras tecnologías (e.g., acelerómetros, giroscopios, etc.) que, combinados, resultan en sistemas muy complejos, cuyos resultados son difíciles de comparar entre sí.

En este capítulo se abordará el análisis de patrones de tecleo en teléfonos móviles mediante múltiples técnicas de aprendizaje automatizado, con el objetivo de establecer una base que permita comparar las ventajas y desventajas de cada uno, de cara a determinar su efectividad, y fijar criterios que justifiquen el uso de unas u otras técnicas de procesamiento en función del escenario de implantación. Para ello se han entrenado modelos de siete sistemas diferentes de aprendizaje automatizado supervisado, utilizado datos del conjunto HMOG (i.e., una de las investigaciones recientes con mayor impacto en el terreno de la autenticación continua basada en biometría conductual móvil). Para generar estos modelos se han elegido los algoritmos de clasificación más utilizados en el estado del arte: *random forest* (RFC), *extra trees classifier* (ETC), *gradiend boosting classifier* (GBC), *k-nearest neighbors* (kNN), *support vector machines* (SVM), *classification and regression tree* (CART) y *naive Bayes*.

Estos modelos han sido puestos a prueba utilizando métricas extraíbles tecla a tecla (i.e., para que con un sólo evento de pulsación se pueda obtener un predictor de la confianza en la identidad del usuario), a saber:

- Tiempo de pulsación: tiempo transcurrido entre que se pulsa, y hasta que se libera una tecla
- Tiempo entre pulsaciones: tiempo transcurrido entre que se pulsa una tecla y se pulsa la siguiente
- Tiempo entre teclas: tiempo transcurrido entre que se libera una tecla y se pulsa la siguiente

Por simplicidad se han utilizado exclusivamente estos tres parámetros, junto con el código identificador de las teclas de origen y destino (i.e., la primera y la segunda tecla pulsadas) tras determinar que, pese a que algunos estudios contemplan el uso de más métricas, estas no son más que combinaciones lineales de las anteriores (e.g., el tiempo entre liberación de teclas es la suma del tiempo entre pulsaciones y el tiempo de pulsación de la segunda tecla).

4.2 Artículo 3

A continuación se expone el artículo 3 del compendio, publicado en la revista *Electronics* de la editorial MDPI, y titulado "*Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics*".

electronics

MDPI

Article

Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics

Luis de-Marcos *, José-Javier Martínez-Herráiz, Javier Junquera-Sánchez, Carlos Cilleruelo and Carmen Pages-Arévalo

Departamento de Ciencias de la Computación, Escuela Politécnica Superior, Universidad de Alcalá, Ctra. Barcelona km 33.6, 28805 Alcalá de Henares, Madrid, Spain; josej.martinez@uah.es (J.-J.M.-H.); javier.junquera@uah.es (J.J.-S.); carlos.cilleruelo@uah.es (C.C.); carmina.pages@uah.es (C.P.-A.)
* Correspondence: luis.demarcos@uah.es

Abstract: Continuous authentication (CA) is the process to verify the user's identity regularly without their active participation. CA is becoming increasingly important in the mobile environment in which traditional one-time authentication methods are susceptible to attacks, and devices can be subject to loss or theft. The existing literature reports CA approaches using various input data from typing events, sensors, gestures, or other user interactions. However, there is significant diversity in the methodology and systems used, to the point that studies differ significantly in the features used, data acquisition, extraction, training, and evaluation. It is, therefore, difficult to establish a reliable basis to compare CA methods. In this study, keystroke mechanics of the public HMOG dataset were used to train seven different machine learning classifiers, including ensemble methods (RFC, ETC, and GBC), instance-based (k-NN), hyperplane optimization (SVM), decision trees (CART), and probabilistic methods (naïve Bayes). The results show that a small number of key events and measurements can be used to return predictions of user identity. Ensemble algorithms outperform others regarding the CA mobile keystroke classification problem, with GBC returning the best statistical results.

Keywords: authentication; authentication technology; mobile phone; data analytics; behavioral biometrics; typing dynamics; keystroke analysis; keystroke patterns

Citation: de-Marcos, L.; Martínez-Herráiz, J.-J.; Junquera-Sánchez, J.; Cilleruelo, C.; Pages-Arévalo, C. Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics. *Electronics* **2021**, *10*, 1622. https://doi.org/10.3390/electronics10141622

Academic Editor: Manohar Das

Received: 20 May 2021
Accepted: 3 July 2021
Published: 7 July 2021

1. Introduction

Mobile phones are rather pervasive today, with the prevalence of mobile phones, devices, and mobile communications increasing continuously. The sheer numbers and ubiquity of mobile devices tell about the necessity to establish methods that guarantee secure operation and communication. Authentication is the process of verifying identity of a system user. Authentication in mobile phones is commonly based on tokens like PIN, gesture patterns, passwords, and, more recently, on biometric-based techniques like fingerprint scans or facial recognition. However, attacks can bypass most authentication methods. PINs and passwords are susceptible to guessing or sniffing or more sophisticated methods like video side-channel attacks [1] or reflection reconstruction [2]. Smudge attacks can bypass patterns [3]. Even biometric systems are susceptible to spoofing [4]. Similar concerns arise for voice-based authentication [5]. Additionally, traditional authentication methods are a one-time process that is usually required to log in or unlock the device. Since mobile devices can also be taken without user permission (e.g., stolen), one-time authentication methods may result in unauthorized use even if the user authentication was initially legitimate.

Continuous authentication (CA) aims to mitigate all these shortcomings by running background processes that continuously monitor the user's interactions and characteristics to determine if the ongoing access is legitimate. Evidence on desktop computers suggests that even simple interactions with the keyboard feature unique individual traits [6]. Interaction with a mobile device is supposed to create a more detailed imprint because postural

preferences [7] and other physiological traits like handgrip [8] come into play. CA is then particularly promising in a mobile scenario, but it also brings additional complications for the implementation since particularities of user interaction with mobile devices must be considered. Machine learning (ML) provides a set of classification algorithms that can tell apart legitimate user events from illegitimate ones, providing a backbone to build user models that can be used to implement CA. Since mobile devices and BYOD policies also bring new threats to organizations, threat analysis and threat intelligence efficiency rely on machine learning approaches' efficient application [9]. ML classifiers used in recent studies include random forests [10], neural networks [11], or even deep learning [12]. However, to the best of our knowledge, there is little evidence comparing and reporting classifiers' performance under the same conditions ([13] is a notable exception). The existing studies differ significantly in critical factors, such as the features selected, their extraction or normalization. The evidence on intrusion detection suggests that feature selection and extraction influence efficiency and effectiveness [14]. The studies also usually focus on tuning the models to beat a given accuracy benchmark for the classifier and dataset under scrutiny. Further, these studies usually compare their results with a small subset of different, and sometimes unrelated, results reported in other studies.

The most common interaction method monitored for CA is keyboard input. Typing determines a unique pattern that has been investigated for traditional keyboards [15] and different variants of mobile keyboards [16]. Standard interaction methods are preferred for CA because they rely on the metrics gathered unobtrusively during regular sessions. Although biometric authentication methods like facial recognition can be used, they usually present several practical problems that designers have to face. Firstly, biometric data demand specific protection and privacy features in systems that deal with them, although specific legal requirements vary depending on the geographical location. Secondly, biometric authentication methods depend on the availability of resources (e.g., cameras) to capture data. The device may deny access resulting in interruptions of the user's regular interaction similarly to other token-based authentication methods. In the mobile environment, modern smartphones provide additional input sensors and can capture user gestures. All these can be combined with keystrokes to provide a lot of data of user interactions that can be used for CA. However, this research body tends to produce ad-hoc solutions that rely on a complex operational process with multiple stages (data gathering, feature extraction, and decision-making) difficult to extend or implement in broader contexts.

This research contributes to knowledge by:

- presenting the results of training and comparing ML CA models based on keystroke mechanics that use substantially fewer features than the current state-of-the-art models but nonetheless offer comparable results.
- showing that a small number of key events and metrics return accurate predictions of the user's identity.

The results are also relevant for practitioners and the broader access control community since ML CA models can be used to implement or feed mobile agents that can respond to incidents. In this way, communication between different agents (e.g., client–server) will be more efficient. Further, our approach also results in user CA models that can be efficiently built, maintained, and updated.

The rest of the paper is structured as follows. Section 2 presents the literature review of CA and keystroke mechanics. Section 3 presents the methodology of the study. The results are presented in Section 4. The paper closes with the discussion and conclusions.

2. Literature Review

Continuous authentication is the process of determining the legitimacy of the user's identity without their active participation. CA contrasts with traditional authentication that usually relies on system credentials provided once to identify the user. CA systems typically run as a background process that gathers information about physical or behavioral properties to determine the identity. The first and most popular method of CA is to use

keyboard interactions [17]. Measurements of keypresses like the down–up or up–down time can be used to define individual patterns. They can be taken for every single key event (usually called monograph features) or for a sequence of two (digraph features) or more keys. The latter facilitates determining the latency of presses and releases between different events. CA models for keystroke dynamics achieve high accuracy with a low false acceptance ratio even for free-text input [18]. The body of study of these techniques is usually called keystroke dynamics or keystroke behavioral biometrics. A systematic literature review of keystroke dynamics can be found in [19].

Given the existing body of research on PC-based keystroke dynamics, it is not surprising that initial works on CA for mobile devices also focused on keyboard events. Seminal works on mobile phone CA focused on keystroke mechanics with a hardware keypad included in the first generations of handset devices [11]. However, with the spread of touchscreen mobile devices, this body of work has been adapted to virtual keyboards as they became commonly available in smartphones. Teh et al. [16] presented a literature review of touch dynamics biometrics for virtual keyboards. They divided the operational process into three stages: data acquisition, feature extraction, and decision-making. The decision-making techniques reported in the literature are probabilistic modeling, cluster analysis, decision trees, support vector machines, neural networks, distance, and other statistical methods.

Further, smartphones provide two additional elements that can be used to capture additional data to feed CA models and processes. Firstly, they include a set of sensors (e.g., an accelerometer, a gyroscope), the input values whereof can be captured at any given moment or event. Second, touchscreens provide the capability to capture user gestures. The input associated with these interactions (e.g., position or pressure) can also be monitored during the gesture. All this additional input provided the ground for the third generation of mobile CA that takes advantage of sensor and gesture data. Sensor-enhanced keystroke mechanics improve gesture-based authentication and traditional keystroke mechanics [20]. Shunwandy et al. presented a literature review on sensor-based authentication, although they focused on healthcare [21], a special sensitive domain for authentication [22]. Experimentation with touch features shows that they provide reliable short-term CA predictions which can be effectively combined with other long-term authentication methods [23]. Hand movement, orientation, and grasp (HMOG) is a set of behavioral biometrics for smartphones introduced by Sitová et al. [24]. It includes two types of features (resistance and stability) that can be used on their own or combined with others (taps, keystrokes, and sensors) for CA. Sitova et al. reported that HMOG outperforms individual sensors. The best results come, however, when HMOG is augmented with tap and keystroke features. Their results also show that HMOG features are particularly suited for CA during walking sessions.

Smith-Creasey and Rajarajan [10] presented a gesture-typing method on mobile phones that can authenticate users for each word. Gesture typing is a different input method in which users press and slide their finger between the characters that form the word that they want to type. Their scheme considers unique aspects of gesture typing, such as redirections and pauses. They reported an error rate of 3.5% for a single-word gesture and 0.8% for three-word gestures. Although this method yields the best results reported in the literature, it relies on an unusual input method. It also requires extracting a significant number of features from gestures and subgestures and undertaking normalization and fusion techniques with extracted data.

However, the current literature focuses on improving CA methods' accuracy by applying a multistage process that usually includes data gathering, feature extraction, normalization, model building, and testing. This process makes it difficult to compare classifiers to the extent that it is questionable whether such complexity presents a substantial improvement. To our knowledge, the only study to approach mobile CA from a comparative perspective has been carried out by Serwadda et al. [13] who reported a dataset and a controlled experiment to compare the performance of ten classifiers for touch gestures

on smartphones. They concluded that logistic regression outperforms other classifiers for vertical strokes. SVM, random forests, and logistic regression returned similar results for horizontal strokes, although they outperformed all the other methods studied.

Since current research relies on a myriad of input data and complex modeling to continuously authenticate mobile phone users, this study sets out to study the feasibility of using lighter CA agents based on metrics from a single input or sensor. This approach results in more scalable CA systems than the current state-of-the-art mobile CA methods, providing acceptable accuracy levels for user prediction. Further, this study also aims to build authentication models that are based on one or a short sequence of events using ML algorithms, and it also compares the accuracy of different ML classifiers.

3. Methodology

For this research, we trained and tested seven ML CA models that can return predictions of user identities for each single keypress event recorded by the soft keyboard of mobile phones. The following subsections report the measurements used in this study, the dataset, and the ML classifiers and metrics used to compare the performance of CA models.

3.1. Measurements of Keystroke Dynamics

The following keystroke mechanics metrics were considered for the mobile CA agent considered for this study (Figure 1): pressingTime, timeReleaseNextPress, and timeBetweenPress. PressingTime is the key hold latency between the press and the release of a given key of the soft keyboard. This measurement is also called down–up time, and it is a key hold feature for each key pressed. TimeReleaseNextPress (up–down time) is the time between the key's release and the following keypress. TimeBetweenPress (down–down time) is the time between the press of a key and the next keypress. Down–down time and up–down time are considered digraph features since they consider two consecutive keypresses. Measurements of single keypresses, like pressingTime, are called unigraph features. All the measurements were taken in milliseconds for each key pressed. Additionally, it is also possible to record the key code of the present key (keyCode) and the key code of the next key pressed (nextKeyCode).

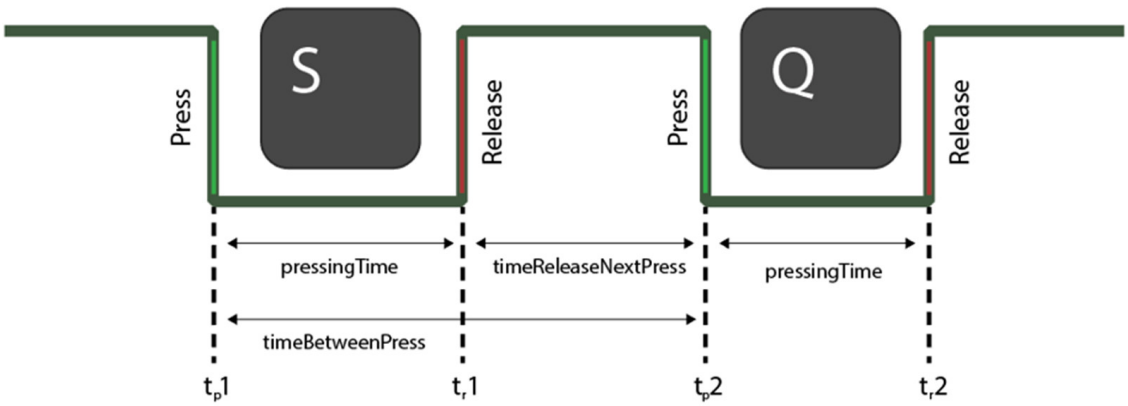

Figure 1. Keystroke mechanics of this study.

3.2. Dataset

The data used in this study come from a public HMOG dataset (http://www.cs.wm.edu/~qyang/hmog.html; accessed on 18 December 2019) [24,25]. A HMOG dataset records interactions of 100 users during 24 sessions (eight reading sessions, eight writing sessions, and eight map navigation sessions). It includes sensor information, touches, gestures, and keypresses on the virtual keyboard. The HMOG dataset recorded raw data for each keypress event, including the timestamp, type (down or up), and key code. For this study, the keypress event information of all the eight writing sessions of the HMOG dataset was

transformed using a Python script that computed pressingTime, timeBetweenPress, and timeReleaseNextPress based on the timestamps and types of keypresses reported in the dataset. The transformed dataset used in this study includes 712,418 keypress events for 100 users (from 4306 to 11,917 events). Descriptive statistics of the variables for all the users are presented in Table 1.

Table 1. Descriptive statistics of measurements for the transformed dataset (n = 712,418).

Measurement	Mean	SE of the Mean	SD	Median
pressingTime	92.82	0.03	28.26	91
timeBetweenPress	455.06	0.60	504.10	309
timeReleaseNextPress	362.24	0.70	504.82	212

Datasets for training ML models were subsequently built for each participant. To do so, each dataset included the user's keystroke events and a random sample of events from other users. Events from the user were labeled as authorized or legitimate (positives), and random events from other users were labeled as unauthorized or malicious (negatives). Each dataset included approximately 50% authorized events and 50% unauthorized events. Table 2 presents the dataset's headers and a few data entries that provide an example to show its structure.

Table 2. Structure of the transformed dataset: headers and a sample of data entries.

Key Code	Pressing Time	Time between Press	Time Release Next Press	Next Key Code	Authorized
32	112	666	554	107	1
107	110	104	403	110	1
110	82	517	435	8	1
8	103	1270	1157	99	1
99	85	935	850	115	0
115	108	17	–91	101	0
101	140	237	97	32	0

3.3. Machine Learning Classifiers

ML models for continuous authentication of users can be implemented using ML classifiers. The second objective of this study is to compare ML algorithms for mobile CA using keystroke dynamics. Since the CA problem is a classification problem that aims to tell apart authorized events from unauthorized events, we focused on classification-supervised algorithms. The algorithms tested in this study included a variety that covers the most common and popular categories of classifiers. Ensemble methods are composed of weaker models independently trained and combined to make an overall prediction. It is a class of algorithms that is rather popular nowadays. This study included three ensemble algorithms: random forest classifier (RFC) [26], extra trees classifier (ETC) [27], and gradient boosting classifier (GBC) [28]. Instance-based algorithms make decisions based on other known instances of the problem considered important or representative, typically using a similarity measure. This class was represented in this study by the k-nearest neighbors (k-NN) algorithm. Hyperplane methods like support vector machines (SVM) compute a mathematical model using a hyperplane that consists of a set of decision boundaries used to classify datapoints. The points are then classified according to the side of the hyperplane in which they fall. Decision tree algorithms build a model of decisions based on the values of attributes in the data. Classification and regression tree (CART) was included in this study. Finally, naïve Bayes was included to represent Bayesian algorithms. For a detailed description of classification algorithms see [29]. An ML model for each of these algorithms was implemented in Python using the scikit-learn module [30].

Crossvalidation with five folds was used to train and test the classifiers. We used the standard target ML metrics to compare ML algorithms' performance: accuracy, precision,

recall, and F1. Accuracy is the ratio between correct predictions and the size of the dataset. Precision measures how many of the predicted positives are true positives. Recall returns how many of the actual positives (true positives + false negatives) the model can predict. Precision should be the target metric when the costs of a false positive are high, while recall is preferred when a false negative is high. F1 represents a balance between precision and recall used when there is an uneven class distribution in the dataset. A false positive may entail a higher cost for CA since it means that an unauthorized person uses the device. A false negative would mean blocking the device or session of authorized users requiring that they authenticate again. The receiver operating characteristic (ROC) curve was also produced for each participant and all classifiers. The area under the curve (AUC) is a summary statistic of the ROC curve representing the probability of ranking a randomly chosen positive instance higher than a randomly chosen negative one. It is representative of how much the model is capable of distinguishing between positives and negatives. Since ML classifiers for the CA problem are binary, we also included the Matthews correlation coefficient (MCC). MCC returns a value between -1 and 1, representing the correlation between the true and the predicted classes. Accuracy is sensitive to class imbalance while the other standard metrics (precision, recall, F1) are asymmetric. MCC is a more reliable statistical metric that produces a high score only if both classes are predicted well, even if one class is disproportionately overrepresented [31].

4. Results

Table 3 shows the average results returned by the different ML classifiers for the CA problem for the 100 users extracted from the HMOG dataset. The results of each metric are also presented graphically in Figure 2. Ensemble algorithms (RFC, ETC, GBC) performed better, with an average of over 70% for most target metrics. The results show high variability between participants, with accuracy ranging between 0.58 and 0.91 across users. Ensemble methods are followed by k-NN, which outperforms SVM. It returns an average accuracy of 0.65, although variability ranges substantially (between 0.56 and 0.89) for ensemble algorithms. SVM returns the worst performance of all classifiers with an average accuracy of 0.59 (from 0.51 to 0.70). Four different kernels were tested (linear, sigmoid, polynomial, and RBF). The radial basis function (RBF) returns substantially better results than others, and it is used for testing and comparison. Naïve Bayes performs similarly to k-NN and CART, and it also shows a considerable variability among users with values ranging between 0.54 and 0.84. The decision tree classifier implementing the CART algorithm returns the second-lowest accuracy measure with an average of 0.63 (from 0.55 to 0.86).

Table 3. Results of ML classifiers for the CA problem. Average of target metrics.

Classifier	Accuracy		Precision		Recall		F1		AUC		MCC	
-	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD
RFC	0.68	0.06	0.71	0.06	0.76	0.07	0.73	0.06	0.72	0.07	0.59	0.12
ETC	0.67	0.06	0.70	0.06	0.74	0.07	0.72	0.06	0.71	0.07	0.57	0.12
GBC	0.71	0.05	0.71	0.06	0.83	0.06	0.76	0.05	0.74	0.07	0.63	0.11
k-NN	0.65	0.06	0.68	0.06	0.74	0.07	0.71	0.06	0.67	0.07	0.48	0.13
SVM	0.59	0.04	0.60	0.05	0.68	0.15	0.61	0.12	0.60	0.05	0.19	0.06
Naïve Bayes	0.64	0.06	0.66	0.07	0.72	0.14	0.72	0.08	0.67	0.08	0.45	0.13
CART	0.63	0.05	0.68	0.06	0.66	0.06	0.67	0.06	0.61	0.06	0.41	0.11

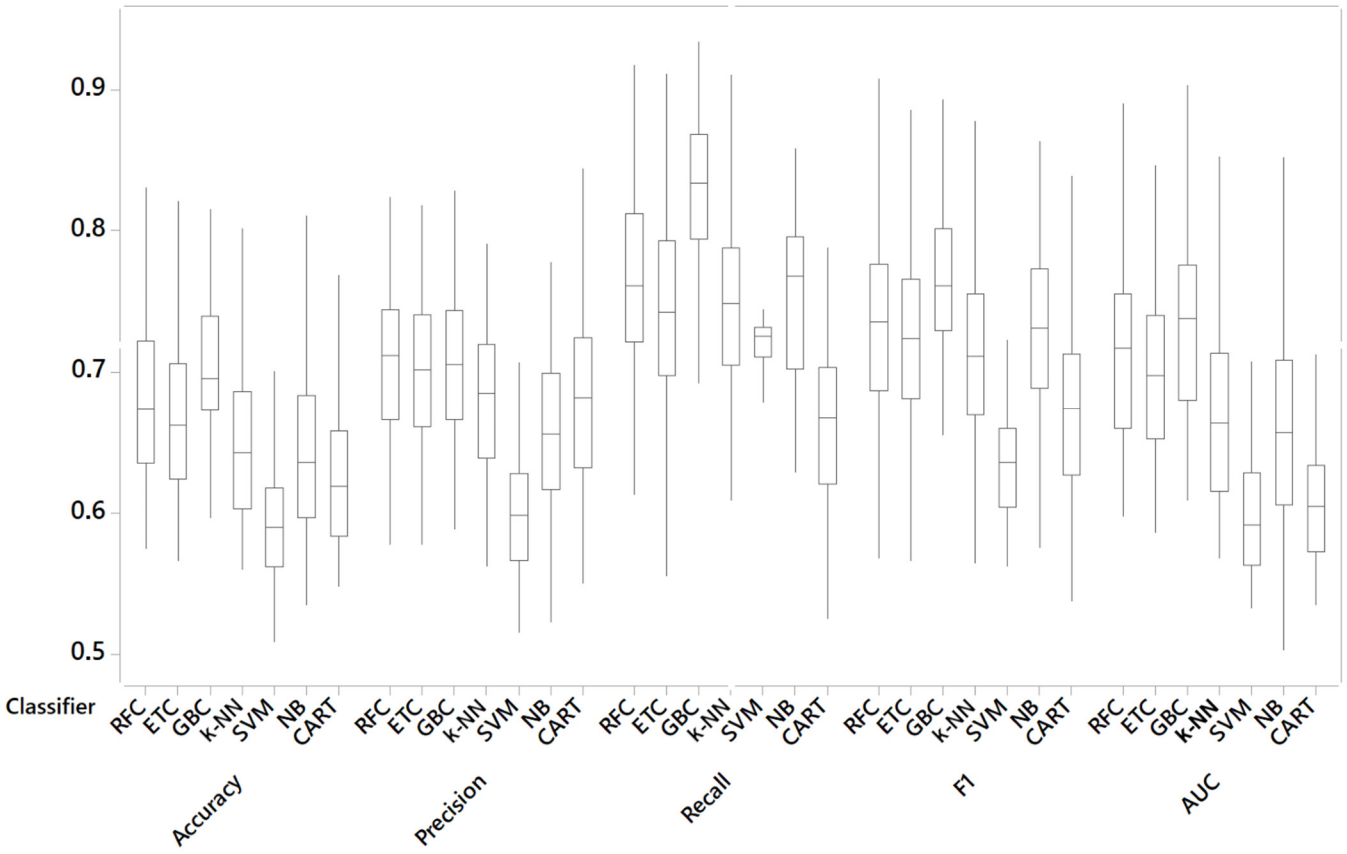

Figure 2. Boxplot of metrics (accuracy, precision, recall, F1, AUC) of ML classifiers for the CA problem.

We run an analysis of variance (ANOVA) to statistically compare the differences between the 100 samples for each classifier. The results showed that the differences were significant across all the metrics: accuracy (F = 45.41, $p < 0.001$), precision (F = 42.81, $p < 0.001$), recall (F = 31.90, $p < 0.001$), F1 (F = 45.99, $p < 0.001$), AUC (F = 57.41, $p < 0.001$), and MCC (F = 169.80, $p < 0.001$). The margin of error was 0.01 for a 95% confidence interval of the means for accuracy, precision, F1, and AUC. The margin of error for recall and MCC was 0.02. Tukey's pairwise comparisons showed that GBC outperformed all the other methods statistically for accuracy and recall. For F1, AUC, and MCC, there were no statistical differences between GBC and RFC, although GBC outperformed all the other classifiers. For precision, there were no statistical differences between the three ensemble methods. Figure 3 presents the confidence intervals for accuracy, showing the differences graphically. GBC performed better, while several other groupings are also observed. Overlapping intervals (for each pair of classifiers) in Figure 3 mean that there were no differences. Non-overlapping intervals mean that there were statistical differences between the two methods.

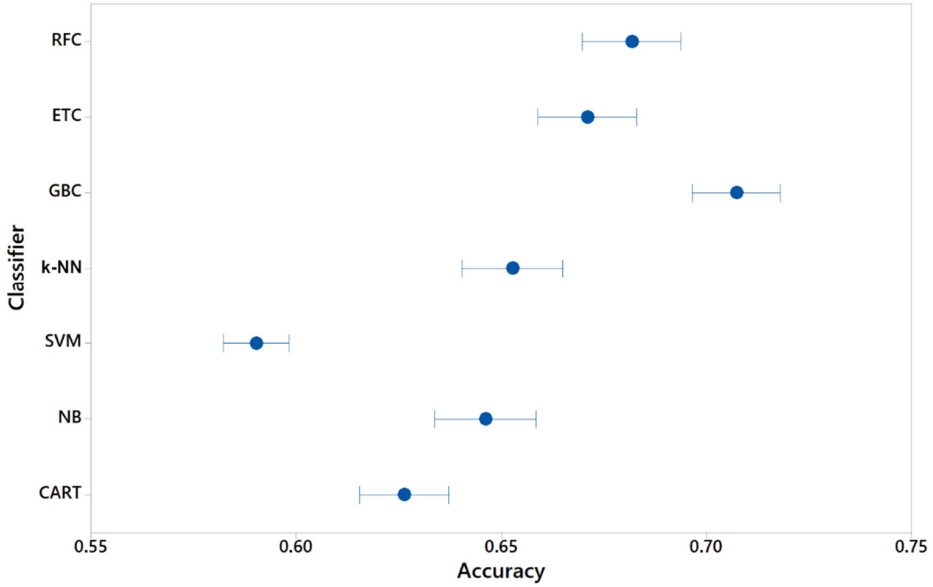

Figure 3. Interval plot of accuracy for all the classifiers (95% confidence interval of the mean). Overlapping between pairs of intervals means that there are no statistical differences.

All the classifiers returned similar scores for all the metrics suggesting that they were not biased towards predicting more false positives than false negatives (or vice versa). GBC and k-NN returned substantially higher values for recall when compared with other metrics. As the recall metric is preferred for the mobile CA problem using keystroke dynamics, the results suggested that GBC was better for the given dataset. The other ensemble classifiers (RFC, ETC) returned a similar result, representing a feasible option to implement ML CA models. As for MCC (Figure 4), the results showed a strong positive correlation (MCC > 0.5) for the three ensemble classifiers. All the other classifiers also returned a moderate positive correlation except SVM that showed no correlation. Figure 5 presents the ROC curve of all the classifiers and the AUC values of an arbitrary user. We can observe that GBC performs better, followed by the other two ensemble classifiers, which perform similarly. Next comes k-NN while CART, naïve Bayes, and SVM perform substantially worse in terms of distinguishing between positives and negatives.

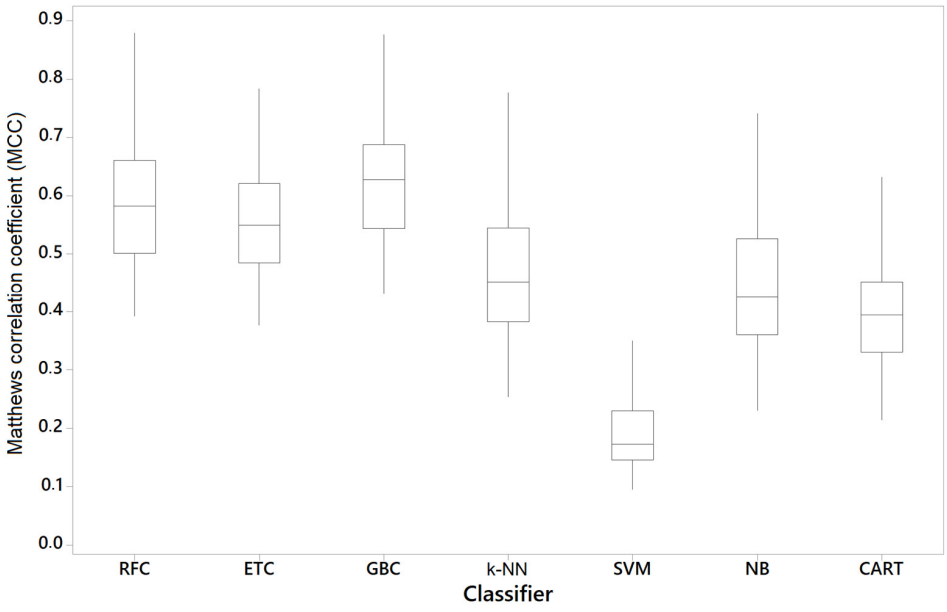

Figure 4. Boxplot of Matthews correlation coefficient of ML classifiers for the CA problem.

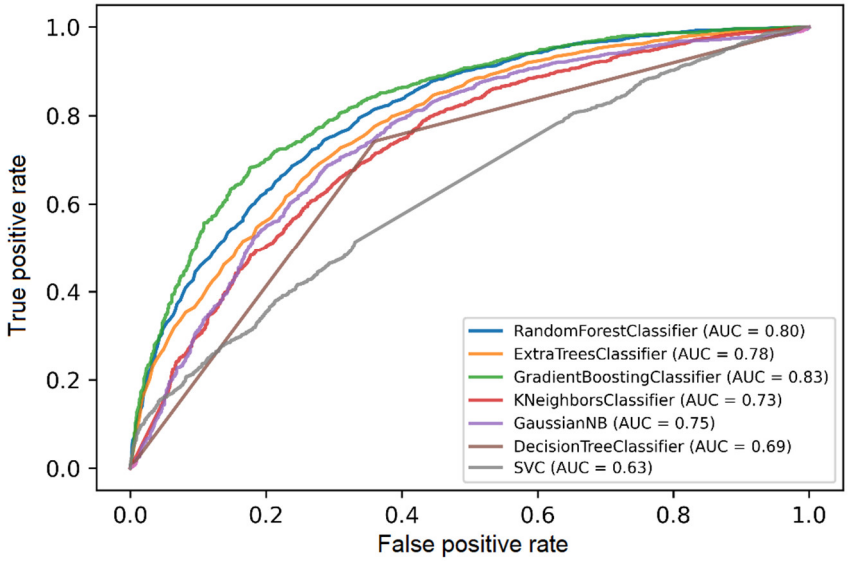

Figure 5. ROC curves of the different classifiers for an arbitrary participant.

Ensemble classifiers (RFC, ETC, and GBC) and the tree classifier (CART) also return the importance of each feature. The most important feature was found to be pressingTime, ranging between 28% and 50% on average for all the classifiers. It was followed by timeReleaseNextPress (14–23%), timeBetweenPress (12–22%), keyCode (12–15%), and nextKeyCode (9–14%). This finding suggests that the three keystroke measurements play a role, each contributing to the final prediction. Previous studies on keystroke mechanics on desktop computers also showed that pressingTime plays a more significant role, which our study also supports for mobile phones. The keys pressed and their sequence in a digraph are the least important features to determine the class to which each event belongs.

The results may suggest that the prediction is not very accurate since even for the best ML classifiers, around 29% of the cases are incorrectly classified. However, every single event (i.e., key pressed) produces a prediction. Therefore, a few individual predictions can be combined to produce a more reliable result, thus mitigating the number of false positives and false negatives. Indeed, current literature suggests using a combination of events for mobile phones or several keypresses (usually in the form of a word or short text) for keystroke dynamics authentication [11]. For this study, the probability of having two false negatives (or positives) in a row is around 0.084, and the probability of having four consecutive false negatives (or positives) is under 0.007 for the best classifier (GBC). Therefore, in the final implementation, a mobile CA agent should respond, e.g., block the device, only if several successive unauthorized predictions or a high percentage are found in recent events. The number of events to consider can be a parameter that can be fine-tuned for each user.

5. Discussion

This paper implemented and compared different ML agent models for CA in mobile environments. Although specific, scalable architectures have been presented [32], to the best of our knowledge, this is the first implementation and testing with specific models for keystroke dynamics using different classifiers on the same dataset. The results suggest that ensemble classifiers (RFC, ETC, and GBC) work better for the problem at hand than instance-based algorithms (k-NN), hyperplane methods (SVM), Bayesian models (naïve Bayes), and decision trees (CART). Notably, GBC outperformed all the other classifiers with statistically significant differences. Ensemble decision classifiers use multiple learning algorithms, typically multiple decision trees, reporting the class that is the mode of all (RFC, ETC). GBC also combines several weak decision trees but using gradient boosting. CART is based on a single strong decision tree classifier that maximizes the information gain at each node. Therefore, we argue that the combination of several weak decision trees

works better for the CA problem and the sample given. Individual decision trees like CART usually face overfitting problems resulting in poorer results for the evaluation set, as we could observe here.

All in all, the difference was around 7–8% for all the target metrics when CART was compared with GBC. Instance-based algorithms (k-NN) make a decision based on individual instances like the majority of a given number of neighbors; k-NN is comparable with ETC and only performs worse than GBC and ETC, suggesting that distance to neighbors can also be a good estimator of the legitimacy of individual key events. This may be particularly useful in environments that require fast response times or have to work with limited training samples since k-NN algorithms are easy to implement, fast, and require fewer data. The drawback of a potential 5% decrease in accuracy can be mitigated by increasing the number of keypresses necessary to make a decision by a mobile agent. Hyperplane methods (SVM) compute the mathematical model that separates most instances when represented as individual points in a hyperspace. SVM returns poor results for the CA problem suggesting that this problem is difficult to model using hyperplanes to classify instances. Our study considered one probabilistic classifier, and we can see that it performed worse than all the ensemble classifiers, although its results were comparable to k-NN and CART. Since Bayesian classifiers consider features to be independent, we argue that this may not be the case for the CA problem using the keystroke measures considered in this study.

When comparing the three ensemble classifiers, we found that GBC outperformed the two others, while no significant differences were found between RFC and ETC. Previous evidence suggests that GBC usually outperforms random forests for classification problems, and our findings suggest that this is also the case for the mobile CA problem with keystroke mechanics. All in all, differences in target metrics were around 4%, and the statistical difference reported here may be caused by sample size. This suggests that gradient boosting with weak decision trees provides a small benefit over ensembles of tree classifiers that return the mode of the forest. The reason may lie in the nature of data, particularly with low dimensionality, since boosting algorithms usually benefit from a large number of features. Differences for the target metrics studied between random forests (RFC) and extra trees (ETC) were marginal and not significant. Extra trees differ from random forests in two aspects. Firstly, random forests select the optimal cutpoint in the splitting process of the tree for each feature, while in extra trees, the point is randomly selected from a uniform distribution of the feature's range. Secondly, ETC uses the whole learning sample to train each tree while RFC uses a sample bootstrap. As results do not return significant differences between RFC and ETC, we argue that the random nature of the splitting point and the set used for training each tree do not yield a substantial benefit in terms of classifier performance. The CA problem and dataset gathered are not affected by the variations coming from the implementation of different ensemble algorithms.

As for the previous studies comparing classifiers, Serwadda et al. found that logistic regression, SVM, and random forest outperformed other classifiers for touch-based CA. They reported error rates ranging between 10% and 21% under different conditions: device orientation (portrait, landscape) and stroke orientation (vertical, horizontal) [13]. Their results contrast with our findings, which suggest that ensemble algorithms perform better, followed by k-NN. In our tests, SVM performed poorly. In Serwadda's results, decision trees and k-NN performed poorly. We did not train a logistic regression classifier. Their approach sampled touch-based CA events at regular intervals, extracting and deriving features from the data acquired, which were subsequently used to train the models. Keystroke dynamics produces data from events that can feed training algorithms directly or after a relatively simple extraction. Such differences can explain why statistical methods work better for touch-based strokes while k-NN works better for keystroke dynamics. Ensemble methods performed well in both cases (although Serwadda et al. only reported the random forest), returning promising results to guide future investigations.

The results also suggest that a small number of keystroke measurements is sufficient to provide accurate predictions of user identity. Our results are comparable to the state-of-the-art studies on PC keystroke dynamics [18]. Clarke and Furnell [11] reported error rates of 8% and 9% for inputs of eleven digits and four digits on mobile phones' hardware keypads. Studies on gesture typing return error rates around 3.5% for one word and under 1% for three words [10]. Our findings also suggest that similar results can be obtained using the soft keyboard's measurements with only a few characters when the user model is trained. This also mitigates the possible effects that typing bursts may have for mobile CA. CA mobile agents can make decisions and take actions even if user interaction takes the form of short bursts. As for training, agents may gather data during users' regular interactions independently of their typing form to get enough interactions to train their models. The effect of fatigue and typing bursts is also an interesting line of future development for mobile CA.

Several previous studies about keystroke dynamics consider additional measurements like the time between releases (also called up–up time) or the total time between the press of the first key and the release of the second key [16]. However, these are just linear combinations of pressingTime and timeReleaseNextPress. We tested this and other linear combinations of the measurements used in this study and did not find any substantial difference. This result suggests that the measurements selected are sufficient to profile most users and that ML methods can handle possible collinearity between variables, thus not benefiting from features that are just linear combinations of others for the CA problem. A possible issue, however, is the high variability returned by all the classifiers. It suggests that there are users for whom no accurate fingerprint can be learned with a given method, as reported in previous studies [33]. This stresses the necessity of combining several inputs and classification methods to authenticate the majority of participants successfully.

The results of the body of work that uses gestures and/or sensors for CA in mobile phones are difficult to compare with our findings given the fundamental differences in the procedure and features used. However, HMOG [24] also considers key events, so stressing the differences can provide additional insights pointing to the benefits of combining both. HMOG uses fewer key events, focusing only on features of single key events (unigraph). Our study uses the HMOG dataset extracting the digraph features that represent the interaction between a keypress and the following. Provided that the lowest error rates in the original HMOG study were found when HMOG was combined with key and tap events, feeding CA models with additional keypress features may improve the accuracy.

A major drawback of our study is that decisions were based on a single key event resulting in relatively low performance, although comparable with the current state of the art as discussed in this section. In the final part of the results, we suggested that several decisions can be combined to get a better insight. Here, we provide an outline of a workable application. Practical implementation can adopt a voting system that can generate a combined trust value and a decision for a given user. The final CA system can use an API that trains and implements several ML models. Each model can still employ different user measurements (e.g., keystroke dynamics) and have a different weight in the final decision. When the CA system collects sufficient information, each model generates a trust value. The trust value can be based on any ML metrics for a sequence of events or a combination of them. Then, the voting takes place. The weight of each vote should be based on the accuracy of the model. For instance, a model with an accuracy of 96% will have more weight on the final decision and trust than a model with an accuracy of 90%. For each user, given the trust (T_i) and the accuracy (P_i), we can use the following weight sum to compute the final trust:

$$T = \frac{\sum_i (T_i \times P_i)}{\sum_i P_i}$$

The voting system outlined here is an ensemble system. Systems based on complementary methods already showed their potential in practical applications, like recommender systems [34], which also describe how to evaluate them.

This study presents other limitations. The participants' representativity and sample size may be a threat to validity since data come from a public dataset of 100 volunteers over eight writing sessions. The original HMOG dataset did not provide substantial information of participants besides gender. We could not assess the effect of possible unbalances in the sample like age, language, or experience with mobile phones, limiting the generalization of our findings. The reduced number of sessions is somehow mitigated by a large number of participants and of events per participant, which facilitate a good statistical representation. Representativity of the sessions is also a limitation since the creators of the HMOG dataset designed these to represent everyday interactions. Research on attack detection shows that unknown attacks are difficult to learn from [35], and as CA usually models impostors as the action of others, CA systems may respond poorly to new attack vectors. Several studies also analyzed the environmental conditions of the interaction, such as posture (e.g., walking, sitting), which our study did not address. Other studies also included device orientation (portrait, landscape), which our study did not analyze either since we considered all the key events of the writing sessions of the original HMOG dataset as equally representative of users' typing interactions. Besides all these limitations, this study establishes the experimental conditions required to make the results of machine learning classifiers comparable, establishing a testbench that can guide future research and practitioners of mobile CA systems.

6. Conclusions

This paper presented an agent model that facilitates the integration and development of CA in mobile devices. Seven different classifiers were then trained and tested using keystroke dynamics captured from mobile devices' soft keyboard events from the HMOG dataset. The results show that all the digraph features used in this study (down–up, up–down, and down–down time) were relevant for the CA classification problem. Ensemble algorithms (RFC, ETC, GBC) performed better, with an average accuracy of around 0.70 for every single key event. GBC outperformed all the other classifiers, and the differences were statistically significant. Naïve Bayes and k-NN returned an accuracy of around 0.65. SVM performed substantially worse than all the other algorithms, suggesting that hyperplane-based classifiers are less appropriate for CA based on keystroke mechanics. The results are relevant to researchers and practitioners aiming to design and implement effective and scalable CA systems.

We plan to analyze energy and resource usage as future work and compare them with the existing studies [24,36]. Other studies also present novel classifiers like artificial immune systems [37] or deep learning models [12], providing additional opportunities for comparison. Evidence on intrusion detection also showed that two-stage systems increase accuracy without compromising efficiency [38]. Keystroke mechanics can also be compared or complemented with other biometric data like facial recognition, fingerprint, or even novel ones like electrocardiogram-based authentication [39]. Similarly, intrasession features (e.g., user's clothes) can be considered as well as other behavioral data gathered from the mobile phone (e.g., apps running). Privacy is also a concern that can be mitigated with pseudonymization and anonymization approaches [40]. Finally, additional research into the number of keystroke events required to train accurate user models can also provide additional insights to researchers and practitioners. From a practical perspective, it may be necessary to deploy mobile CA systems avoiding the cold start problems inherent to ML solutions. There is also the possibility of users having different models under different conditions or devices, so intersession CA is also a promising research area.

Author Contributions: Conceptualization, L.d.-M. and J.-J.M.-H.; Data curation, J.J.-S. and C.C.; Formal analysis, J.J.-S. and C.C.; Funding acquisition, J.-J.M.-H.; Methodology, L.d.-M.; Project administration, L.d.-M.; Resources, C.P.-A.; Supervision, L.d.-M., J.-J.M.-H. and C.P.-A.; Validation, J.J.-S., C.C. and C.P.-A.; Writing—original draft preparation, L.d.-M., J.J.-S. and C.C.; Writing—review and editing, J.-J.M.-H. and C.P.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This project received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 826284.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to the fact that all data used in this research are from a public external dataset. This study did not collect any new personal or sensitive information from any participant.

Informed Consent Statement: Participant consent was waived because all data comes from a public dataset. Description of participants and consent, if applicable, can be found in original the dataset. Please refer to the dataset source in Data Availability Statement below for more information.

Data Availability Statement: The data used in this research are from the HMOG dataset (http://www.cs.wm.edu/~qyang/hmog.html; accessed on 18 December 2019) licensed by The College of William and Mary for noncommercial, educational, and research purposes only. The College of William and Mary does not bear any responsibility for the analysis or interpretation of the HMOG dataset presented in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shukla, D.; Kumar, R.; Serwadda, A.; Phoha, V.V. Beware, Your hands reveal your secrets! In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 904–917.
2. Xu, Y.; Heinly, J.; White, A.M.; Monrose, F.; Frahm, J.-M. Seeing double: Reconstructing obscured typed input from repeated compromising reflections. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 1063–1074.
3. Aviv, A.J.; Gibson, K.; Mossop, E.; Blaze, M.; Smith, J.M. Smudge on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies, WOOT 10, Washington, DC, USA, 9 August 2010.
4. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.R.; Pedrini, H.; Falcão, A.X.; Rocha, A. deep representations for iris, face, and fingerprint spoofing detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 864–879. [CrossRef]
5. Bonastre, J.-F.; Bimbot, F.; Boe, L.-J.; Magrin-Chagnolleau, I. Person authentication by voice: A need for caution. In Proceedings of the 8th European Conference on Speech Communication and Technology, EUROSPEECH 2003-INTERSPEECH 2003, Geneva, Switzerland, 1–4 September 2003.
6. Banerjee, S.; Woodard, D.L. Biometric Authentication and identification using Keystroke dynamics: A survey. *J. Pattern Recognit. Res.* **2012**, *7*, 116–139. [CrossRef]
7. Azenkot, S.; Zhai, S. Touch behavior with different postures on soft smartphone keyboards. In Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services, San Francisco, CA, USA, 21–24 September 2012; pp. 251–260.
8. Kim, K.-E.; Chang, W.; Cho, S.-J.; Shim, J.; Lee, H.; Park, J.; Lee, Y.; Kim, S. Hand grip pattern recognition for mobile user interfaces. In Proceedings of the 18th Conference on Innovative Applications of Artificial Intelligence, Boston, MA, USA, 16–20 July 2006; Volume 2, pp. 1789–1794.
9. Ibrahim, A.; Thiruvady, D.; Schneider, J.-G.; Abdelrazek, M. The challenges of leveraging threat intelligence to stop data breaches. *Front. Comput. Sci.* **2020**, *2*. [CrossRef]
10. Smith-Creasey, M.; Rajarajan, M. A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Comput. Secur.* **2019**, *83*, 140–150. [CrossRef]
11. Clarke, N.L.; Furnell, S.M. Authenticating mobile phone users using keystroke analysis. *Int. J. Inf. Secur.* **2007**, *6*, 1–14. [CrossRef]
12. Volaka, H.C.; Alptekin, G.; Basar, O.E.; Isbilen, M.; Incel, O.D. Towards continuous authentication on mobile phones using deep learning Models. *Procedia Comput. Sci.* **2019**, *155*, 177–184. [CrossRef]
13. Serwadda, A.; Phoha, V.V.; Wang, Z. Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms. In Proceedings of the IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 29 September–2 October 2013; pp. 1–8.
14. Siddiqi, M.A.; Pak, W. Optimizing filter-based feature selection method flow for intrusion detection system. *Electronics* **2020**, *9*, 2114. [CrossRef]
15. Bours, P.; Mondal, S. Continuous Authentication with Keystroke Dynamics. In *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*; Zhong, Y., Deng, Y., Eds.; Science Gate Publishing: Thrace, Greece, 2015; Volume 2, pp. 41–58.
16. Teh, P.S.; Zhang, N.; Teoh, A.B.J.; Chen, K. A survey on touch dynamics authentication in mobile devices. *Comput. Secur.* **2016**, *59*, 210–235. [CrossRef]
17. Shepherd, S.J. Continuous authentication by analysis of keyboard typing characteristics. In Proceedings of the European Convention on Security and Detection, Brighton, UK, 16–18 May 1995; pp. 111–114.
18. Ahmed, A.A.; Traore, I. Biometric recognition based on free-text keystroke dynamics. *IEEE Trans. Cybern.* **2014**, *44*, 458–472. [CrossRef]
19. Pisani, P.H.; Lorena, A.C. A systematic review on keystroke dynamics. *J. Braz. Comput. Soc.* **2013**, *19*, 573–587. [CrossRef]

20. Giuffrida, C.; Majdanik, K.; Conti, M.; Bos, H. I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Egham, UK, 10–11 July 2014; pp. 92–111.
21. Shuwandy, M.L.; Zaidan, B.B.; Zaidan, A.A.; Albahri, A.S. Sensor-Based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review. *J. Med. Syst.* **2019**, *43*, 33. [CrossRef] [PubMed]
22. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications. *Secur. Commun. Netw.* **2019**, *2019*, 3263902. [CrossRef]
23. Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 136–148. [CrossRef]
24. Sitová, Z.; Šeděnka, J.; Yang, Q.; Peng, G.; Zhou, G.; Gasti, P.; Balagani, K.S. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 877–892. [CrossRef]
25. Yang, Q.; Peng, G.; Nguyen, D.T.; Qi, X.; Zhou, G.; Sitová, Z.; Gasti, P.; Balagani, K.S. A multimodal data set for evaluating continuous authentication performance in smartphones. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, Memphis, TN, USA, 3–6 November 2014; pp. 358–359.
26. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]
27. Geurts, P.; Ernst, D.; Wehenkel, L. Extremely randomized trees. *Mach. Learn.* **2006**, *63*, 5–32. [CrossRef]
28. Friedman, J.H. Greedy Function Approximation: A Gradient Boosting Machine. *Ann. Stat.* **2001**, *29*, 1189–1232. [CrossRef]
29. Hastie, T.; Tibshirani, R.; Friedman, J. *The Elements of Statistical Learning. Data Mining, Inference and Prediction*; Springer: New York, NY, USA, 2009.
30. Pedregosa, F.; Varoquaux, G.; Gramfort, A.; Michel, V.; Thirion, B.; Grisel, O.; Blondel, M.; Prettenhofer, P.; Weiss, R.; Dubourg, V.; et al. Scikit-Learn: Machine learning in Python. *J. Mach. Learn. Res.* **2011**, *12*, 2825–2830.
31. Chicco, D.; Jurman, G. The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genom.* **2020**, *21*, 6. [CrossRef]
32. Junquera-Sánchez, J.; Cilleruelo-Rodríguez, C.; de-Marcos, L.; Martínez-Herráiz, J.J. JBCA: Designing an adaptative continuous authentication architecture. In *Advances in Physical Agents II*; Bergasa, L.M., Ocaña, M., Barea, R., López-Guillén, E., Revenga, P., Eds.; Springer International Publishing: Madrid, Spain, 2020; pp. 194–209.
33. Gascon, H.; Uellenbeck, S.; Wolf, C.; Rieck, K. Continuous authentication on mobile devices by analysis of typing motion behavior. In Proceedings of the Security 2014—Security, Protection and Reliability, Vienna, Austria, 19–21 March 2014; pp. 1–12.
34. Bell, R.M.; Koren, Y. Lessons from the Netflix prize challenge. *SIGKDD Explor. Newsl.* **2007**, *9*, 75–79. [CrossRef]
35. Al-Zewairi, M.; Almajali, S.; Ayyash, M. Unknown security attack detection using shallow and deep ANN classifiers. *Electronics* **2020**, *9*, 2006. [CrossRef]
36. Basar, O.E.; Alptekin, G.; Volaka, H.C.; Isbilen, M.; Incel, O.D. Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. *Procedia Comput. Sci.* **2019**, *155*, 185–192. [CrossRef]
37. Aljohani, N.; Shelton, J.; Roy, K. Continuous authentication on smartphones using an artificial immune system. In Proceedings of the 28th Modern Artificial Intelligence and Cognitive Science, Fort Wayne, IN, USA, 28–29 April 2017; pp. 171–174.
38. Reyes, A.A.; Vaca, F.D.; Castro Aguayo, G.A.; Niyaz, Q.; Devabhaktuni, V. A machine learning based two-stage wifi network intrusion detection system. *Electronics* **2020**, *9*, 1689. [CrossRef]
39. Zhang, Y.; Gravina, R.; Lu, H.; Villari, M.; Fortino, G. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *J. Netw. Comput. Appl.* **2018**, *117*, 10–16. [CrossRef]
40. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system. *Int. J. Environ. Res. Public Health* **2019**, *16*, 1490. [CrossRef] [PubMed]

4.3 Resumen de los resultados del artículo 3

Se ha abordado el estudio de siete algoritmos no supervisados de clasificación aplicados a un conjunto de datos de tecleo, y de cómo estos pueden contribuir a la biometría conductual, obteniendo diferentes métricas que permitirán evaluar su idoneidad en diferentes escenarios en los que se pueda requerir la autenticación continua del usuario.

Los resultados evidencian que es posible inferir la identidad de un usuario con pocos eventos de tecleo, con especial prevalencia mediante el uso del algoritmo GBC; pero también que la eficacia del sistema, utilizando exclusivamente eventos de pulsación aislados (i.e., haciendo una evaluación, tecla a tecla, de manera individualizada), son algo peores que los reflejados por la literatura. Si se fuesen utilizar este modelo en un sistema de control de accesos, se sugiere la aplicación de varias iteraciones de evaluación, e.g., implementando un sistema de votación para diferentes algoritmos, antes de extraer un veredicto final.

Mostrando, por cada algoritmo, diferentes métricas de rendimiento (e.g., *accuracy*, *precision*, *recall*, etc.) necesarias para la evaluación de escenarios concretos (e.g., si se buscase evaluar la identidad a lo largo de la sesión de trabajo sin perturbar al usuario, es decir, que la tasa de falso rechazo sea baja, nos centraríamos en el *recall*), se cumple, por lo tanto, uno de los principales objetivos, que es el de extraer resultados experimentales homologables entre distintas técnicas de aprendizaje automático, que sirvan de base para futuras investigaciones en el ámbito de la autenticación continua.

Expuestos los tres artículos, y analizadas sus contribuciones, en el próximo capítulo se discutirán los principales resultados de cara a obtener una síntesis que dé respuesta los objetivos de investigación planteados al comienzo de esta tesis.

Capítulo 5

Resultados y discusión

Una vez presentados los tres artículos que forman el compendio, en este capítulo se discutirán los resultados obtenidos. A continuación se expondrá la relación que cada uno de estos artículos guarda con los objetivos de investigación de la tesis.

5.1 Artículo 1. Revisión sistemática de la literatura sobre autenticación continua

Se realiza una búsqueda metódica del término "autenticación continua" en 6 bases de datos científicas, extrayendo de cada una los 20 artículos de mayor impacto, resultando un total de 120. Con el objetivo de evitar sesgos se han definido una serie de criterios de inclusión y exclusión, y criterios de calidad, que permiten determinar si un artículo entra a formar parte del estudio, e.g.: sólo investigaciones primarias con revisión por pares, sólo artículos que documenten experimentación, etc. Tras eliminar resultados duplicados, y aplicar estos criterios, restan 30 artículos. Con ellos, se tratará de responder a las preguntas de investigación planteadas, extrayendo los siguientes datos:

- Entidad cuya identidad se va a evaluar: i.e., qué se pretende identificar a través de la autenticación continua
- Plataforma sobre la que se va a implantar el sistema: ordenador, teléfono móvil, etc.
- Método, o periférico, utilizado para obtener los datos que permiten modelar la entidad a evaluar.
- Métodos para procesar los datos obtenidos, o identificar; y para evaluar posteriormente la identidad, o autenticar.
- Rendimiento, en el ámbito del control de accesos, de la solución propuesta.
- Reproducibilidad: complejidad del experimento, y existencia de conjuntos de datos públicos.

En el artículo se extraen otros datos que permiten guiar el análisis del estado del arte, o ayudan a matizar los resultados, pero estos son los principales parámetros que contribuyen a alcanzar los objetivos de la investigación.

Para empezar a dibujar la respuesta al primer objetivo de investigación de esta tesis (i.e., OI1) definiremos la autenticación continua como el conjunto de métodos de obtención y tratamiento de datos, que permiten evaluar la identidad de una entidad sin su participación activa. Es decir, no se restringe a sistemas de autenticación, ni mucho menos a sistemas de autenticación periódica.

Concretemos qué significa no restringirse a la autenticación: evaluar la identidad significa identificar (i.e., determinar que la identidad de una entidad corresponde a una conocida previamente), pero también detectar fraude y rechazar suplantaciones, aun no teniendo la capacidad de asociar unívocamente la entidad que opera a una identidad concreta conocida. Esto define una de las primeras dimensiones de la autenticación continua: la de la singularidad, o la capacidad que tiene el sistema para identificar unívocamente a una entidad. En función del caso de uso, el requisito de singularidad se traduce en reducir la tasa de falsa aceptación al mínimo. En escenarios en los que el sistema de control de accesos deba ser adaptativo, una singularidad baja no carece de utilidad, porque sí puede ayudar a detectar situaciones de riesgo y desplegar otras medidas.

No requerir de participación activa quiere decir que: 1.- el sistema debe operar de forma transparente, sin que la entidad que opera tenga que realizar una acción concreta para satisfacer la autenticación continua; pero también, 2.- que se debe poder prescindir de una fase de registro. Por lo tanto, siendo estrictos, quedarían fuera sistemas basados en secretos precompartidos. Esto se traduce en los requisitos de aceptabilidad, muy relacionado con la usabilidad, pero enfocado en que la tasa de falso rechazo se mantenga prácticamente nula; y de colectibilidad.

Para que la autenticación continua pueda convivir con otros sistemas en un dispositivo, sin que eso suponga una disminución del rendimiento del resto de procesos, deben establecerse requisitos de eficiencia. Por otro lado, si se buscase utilizar esta aproximación como reemplazo de la autenticación clásica, además de una alta singularidad, y universalidad, es necesario que cumpla con criterios de permanencia; además de resistencia probada a ataques activos, a los que se presupone que puede estar expuesto cualquier sistema de control de accesos, lo que en la literatura se conoce como resistencia a burla (traducción de *mocking rate*).

La entidad por excelencia a autenticar es el ser humano, pero también hay estudios que abordan la autenticación continua de máquinas mediante patrones lógicos, y a través de sistemas más complejos, como análisis de patrones electromagnéticos.

La plataforma más abordada es el teléfono móvil. Uno de los motivos es su implantación en la sociedad, y la gran cantidad de elementos que permiten obtener datos conductuales: sensores, cámara, periféricos virtuales, etc. Otro hecho que motiva el uso de autenticación

continua es su vulnerabilidad frente a robo, y su deslocalización, que hacen de el teléfono móvil un activo que requiere medidas de seguridad adicionales.

Esto se traduce también en que los métodos más estudiados para obtener datos de la entidad a evaluar, sean aquellos presentes en los teléfonos móviles: pantallas táctiles, sensores electrónicos, y el teclado virtual. La conectividad de estos dispositivos también los involucra en otras investigaciones que, si bien pueden aplicarse a cualquier plataforma, guardan una estrecha relación con los teléfonos móviles y los *wearables* sanitarios, pues permiten obtener electrocardiogramas, patrones de actividad física, y otros biométricos.

Aunque existen algunas aproximaciones estadísticas triviales, el procesado masivo de datos para conseguir la autenticación continua pasa, necesariamente, por el uso de algoritmos propios del aprendizaje automatizado. Así, las dos grandes aproximaciones son el uso de algoritmos de clasificación, cuando los datos pueden serializarse y ser normalizados de alguna forma; o el uso de algoritmos de preprocesamiento y filtrado, para trabajar con redes neuronales, cuando se hace uso de imágenes. Aunque, como veremos más adelante en los resultados de nuestro estudio experimental, no es lo que ofrece mejor rendimiento, gran parte de la literatura aborda el procesado de datos mediante SVM (*Support Vector Machine*). Otro aspecto relevante es que prácticamente todas las soluciones adoptadas parten de la necesidad de entrenar con datos de varios usuarios, para poder evaluar la identidad de uno solo.

Los algoritmos de aprendizaje automatizado, y, en concreto, los de clasificación, cuentan con métricas para evaluar su rendimiento. Estas métricas parten de un análisis estadístico en el que se mide cuántas veces la clasificación considera un elemento como positivo (i.e., perteneciente a una clase concreta) o negativo, evaluando cuántas de estas veces la clasificación se ha producido de forma correcta. Así nos encontraremos con verdaderos y falsos positivos, para hacer alusión a las veces que un elemento ha sido clasificado como positivo correcta o incorrectamente, respectivamente; y verdaderos y falsos negativos. Estas métricas permiten obtener indicadores de calidad del sistema como las tasas de *precision*, *recall* y *F1-score*; que no son más que diferentes ratios entre verdaderos y falsos positivos y negativos. Desarrollaremos más la implicación de estas métricas en los resultados del artículo 3 (ver Sección 5.3).

En el caso de la autenticación continua debemos tener en cuenta ciertas peculiaridades en el momento de evaluar una aproximación. Por un lado, la precisión a la hora de diferenciar un individuo del resto suele estar reñida con la flexibilidad lidiando con posibles errores de medición, imprecisiones del modelo, etc. Es decir, cuánto más estricto es el modelo, más seguro será frente a suplantaciones, pero rechazará con mayor probabilidad a los usuarios legítimos cuando la medición de su identidad no se produzca en condiciones óptimas. Traducido a las métricas, se buscará un compromiso entre la ratio de verdaderos positivos, o TPR (del inglés *True Positive Rate*), inversa de la ratio de falsos negativos (FNR); y la de falsos positivos (FPR).

En el ámbito del control de accesos, sin embargo, se prefiere el uso de los términos aceptación y rechazo, en lugar de positivos y negativos; por lo que se suele trabajar con TAR Y FAR (respectivamente, *True Acceptance Rate* y *False Acceptance Rate*). Cuando, evaluando diferentes umbrales de clasificación, ambas métricas se igualan, se obtiene la "tasa de error igual", o EER, del inglés *Equal Error Rate*. Este indicador, que corresponde al valor del FAR en dicho punto, indica cuál debe ser la configuración óptima del modelo, permitiendo la autenticación sin ser demasiado laxo, ni demasiado estricto. Normalmente se aborda este análisis gráficamente mediante curvas ROC [55], o mediante curvas DET (del inglés *Detection Error Tradeoff*)). Numéricamente, a valores de EER más bajos, mayor calidad tiene el modelo. En las investigaciones analizadas, este ratio nunca supera el 0,30, y suele ser prácticamente nulo, aunque siempre bajo condiciones óptimas de laboratorio.

Poniendo el foco en las capacidades concretas de la autenticación continua para el control de acceso, y al margen de la eficacia de los modelos, la singularidad y la permanencia siguen siendo un reto por abordar. Prácticamente ninguna de las investigaciones abordadas evidencia capacidades para autenticar usuarios a lo largo de diferentes sesiones de trabajo.

5.2 Artículo 2. Autenticación dinámica mediante el uso de secretos precompartidos

El segundo artículo presenta un método dinámico para dotar de seguridad adicional a los sistemas de *port-knocking*, y protegerlos frente a adversarios con capacidad de interceptación de comunicaciones. Se busca filtrar las conexiones que llegan al servidor desde los distintos terminales, permitiendo sólo aquellas que han demostrado conocer una secuencia de golpeo de puertos.

La motivación de este trabajo parte de un escenario en el que se ha implantado el sistema de *port-knocking* dentro de un entorno que permite al adversario escuchar las comunicaciones, y, por lo tanto, obtener la secuencia de golpeo. Manteniendo la consonancia con la definición formal enunciada en la sección anterior, este mecanismo, además de encajar técnicamente en el ámbito de la autorización, parte de un secreto precompartido, y por lo tanto no sería una tecnología de autenticación continua. Pero sí cuenta con elementos que lo enfrentan a los problemas que esta afronta: debe evitar suplantaciones derivadas de conocer las credenciales del usuario legítimo (en este caso, la secuencia de golpeo), y hacerlo de una forma que no entorpezca el uso legítimo. Formalizándolo, además de la permanencia, el sistema debe cumplir con el requisito de resistencia a burla, y ser altamente usable.

Mediante el empleo de códigos TOTP se consigue un sistema dinámico utilizando una tecnología que ya se encuentra ampliamente implantada en la industria (e.g., puede ge-

nerarse con aplicaciones como Microsoft Authenticator), que además se sostiene sobre algoritmos criptográficos seguros. Se añade así una barrera adicional a la autenticación, que permitiría, además, evitar impactos directos de ataques de día cero contra el servicio protegido. Este ejemplo pone de manifiesto la relevancia de utilizar un enfoque de defensa en profundidad para proteger el sistema, en coherencia con el segundo objetivo de investigación formulado en la tesis (ver OI2).

Desde el punto de vista de los adversarios, obtendríamos las siguientes garantías de protección para la comunicación:

- Un adversario pasivo, "honesto pero curioso", podría realizar ataques de repetición, pero como máximo durante los 30 segundos que dura la ventana de tiempo hasta la generación de un nuevo código
- Un adversario dinámico *online*, corriendo en tiempo polinómico, no sería capaz de obtener la secuencia; y sólo podría tratar de suplantar al usuario legítimo explotando otros ámbitos de la red (e.g., ataques relacionados con el encaminamiento de los paquetes, del tipo del *ARP spoofing*).
- Un adversario dinámico *offline*, que hubiese obtenido una secuencia de golpeo, no podría obtener el secreto precompartido con el que se generan los códigos TOTP sin encontrar un fallo en los algoritmos criptográficos subyacentes (e.g., rompiendo HMAC, SHA1, etc.).

El mecanismo propuesto contribuye a la seguridad del sistema, siguiendo un enfoque de defensa en profundidad. Robustece, eminentemente, los elementos de protección de redes locales de comunicación basados en *port-knocking*, y otorga resistencia en cualquier otro ámbito donde se tenga que hacer frente a adversarios con acceso a los flujos de datos. Aunque determinados escenarios, como los relacionados con eventuales denegaciones de servicio realizadas por un adversario dinámico *online*, deben ser evaluados para implantar las mitigaciones oportunas en la implementación concreta, el principal riesgo al que se enfrenta el sistema de información protegido se encuentra en el dispositivo que almacena el secreto precompartido.

Si fuese robado el secreto precompartido, con el que se generan las secuencias de golpeo, o un adversario tuviese acceso al dispositivo en el que se generan, el servidor quedaría expuesto de nuevo. Este último supuesto, en el que el atacante tiene acceso físico al dispositivo, es bastante común: por extravío, robo, o simplemente porque un operador se ausente de su puesto y descuide el dispositivo desbloqueado (i.e., autenticado). Persistiendo con la defensa en profundidad, la protección del servidor requerirá implantar medidas que garanticen que la identidad de quien opera legítimamente con los sistemas terminales, sigue siendo la misma hasta el final de la sesión de trabajo (i.e., autenticación continua).

La debilidad expuesta ayuda a esclarecer la diferencia entre un sistema basado en secretos precompartidos, y un verdadero sistema de autenticación continua sustentado

en datos de biometría conductual. Utilizar autenticación continua para proteger, tanto el dispositivo que custodia el secreto precompartido, como cualquier otro que tenga que ser operado por un usuario, habilitará la ejecución de medidas de respuesta de forma adaptativa. Por ejemplo, asegurando la identidad del operador legítimo, o detectando una suplantación para bloquear el dispositivo a tiempo, quedaría asegurado el último eslabón de la cadena de elementos que conecta el activo remoto con el operador (contribuyendo a dar respuesta al OI2).

5.3 Artículo 3. Estudio de sistemas de autenticación continua basados en biometría conductual

Partiendo de las debilidades detectadas en el artículo anterior, y tras evidenciar en el estudio sistemático de la literatura que los teléfonos móviles son los dispositivos más susceptibles de mejorar su seguridad mediante la autenticación continua, para satisfacer el objetivo de investigación 3a, centramos nuestro último artículo en esta plataforma. El estudio de la literatura arroja una gran cantidad de publicaciones centradas en dispositivos móviles, y muchas de ellas se centran en el uso de teclados virtuales, pero los criterios de evaluación no son uniformes, y no suelen fijar objetivos de seguridad en el control de accesos. Este tercer artículo incidirá también en el objetivo de investigación 3 de la tesis, ayudando a establecer una base que sirva de apoyo a la toma de decisiones en materia de autenticación continua, siendo el primer estudio en el que se abordan diferentes clasificadores sobre el mismo conjunto de datos.

El artículo parte del conjunto de datos de HMOG [41]. En este conjuto de datos se recogen eventos de interacción de 100 sujetos con un dispositivo móvil. Entre estos eventos encontramos datos del acelerómetro, eventos de tecleo, gestos en pantalla, etc.; a lo largo de ocho sesiones de trabajo en las que los participantes debían escribir, al menos, 250 caracteres. Para entrenar los clasificadores con nuestras propios datos característicos, procesamos los datos de HMOG y extraemos por cada evento de pulsación:

- *pressingTime*: tiempo transcurrido desde que se pulsa la tecla hasta que se libera.
- *timeBetweenPress*: tiempo transcurrido entre la pulsación de una tecla y la pulsación de la siguiente.
- *timeReleaseNextPress*: tiempo transcurrido desde que se libera una tecla hasta que se presiona la siguiente.

Con cada uno de los 100 sujetos evaluados se ha generado un conjunto de registros propio, al que se ha añadido una columna adicional que indica si el registro (i.e., las tres características anteriores) pertenece a la sesión del usuario, o pertenece a los datos

generados por otro. El conjunto de datos del usuario contendrá un 50 % de datos legítimos, y otro 50 % de datos extraídos aleatoriamente de otros usuarios.

Finalmente, los datos han sido procesados con los 7 algoritmos supervisados de clasificación más utilizados [56], utilizando la implementación de `scikit-learn` [57], y evaluando las siguientes métricas de rendimiento:

1. *accuracy*: ratio de predicciones correctas, positivas o negativas.

$$\frac{TP + TN}{(TP + TN + FP + FN)}$$

2. *precision*: relación entre eventos positivos identificados correctamente (i.e., TP), y todos los eventos identificados como positivos.

$$\frac{TP}{(TP + FP)}$$

3. *recall*: equivalente a la tasa de verdaderos positivos (i.e., TPR), determina la capacidad del modelo para detectar valores positivos.

$$\frac{TP}{(TP + FN)}$$

4. *F1*: media armónica entre *precision* y *recall*, que describe el equilibrio entre falsos positivos y falsos negativos.

$$\frac{2 * precision * recall}{(precision + recall)}$$

Cuanto más cercanos a 1 sean los resultados de estas tasas, más precisión mostrará el algoritmo, pero cada una de ellas presenta particularidades. La precisión indica cómo de bueno es un algoritmo evitando falsos positivos. En el control de accesos esto se traduce en la capacidad del algoritmo para evitar la burla, y que un adversario no sea capaz de engañarlo haciéndose pasar por el operador legítimo. Es un aspecto crítico cuando hablamos de autenticación, pero la autenticación continua puede permitirse no destacar en esta métrica.

Sin embargo, la tasa de *recall*, que muestra la sensibilidad del algoritmo a los datos genuinos, y contra los falsos negativos, no sólo nos dará una percepción del rendimiento del algoritmo, sino que sentenciará si un algoritmo es o no apto para la autenticación continua. En un sistema de autenticación, por ejemplo, no supondría un problema muy

grave introducir varias veces la huella dactilar si no consigue identificarnos; pero uno de los requisitos de la autenticación continua es que no debe interferir en la sesión de trabajo. Aún a costa de sacrificar la detección de suplantaciones, con el consiguiente incremento de la tasa de falsa aceptación (i.e., FAR), el *recall* debe ser lo suficientemente alto como para que nunca se interrumpa una sesión de trabajo indebidamente.

Finalmente, partiendo de la comparación entre FPR y TPR de la curva ROC, la métrica AUC nos permitirá comparar la calidad de los algoritmos en términos generales; y determinar el umbral óptimo a la hora de clasificar en positiva o negativa la identidad del usuario (i.e., ser más laxo, o más estricto), sintetizando el EER.

Los resultados evidencian que, con pocos eventos, se puede dar una predicción de la identidad del usuario. El algoritmo GBC obtiene, de media, los mejores resultados en todas las métricas evaluadas. Además, es el único cuyo *recall* supera el 80 %, por lo que sería el más adecuado de los 7 para un sistema de autenticación continua; seguido por los algoritmos RFC y ETC, con un *recall* del 68 % y un 74 %, respectivamente. Aunque el *recall* de k-NN es igual que el de ETC, tanto el *accuracy* como la precisión son ligeramente peores.

Estudiando el resto de métricas, los algoritmos ETC y k-NN obtienen resultados semejantes. Aunque los resultados arrojados por ETC aventajan sensiblemente a los de k-NN, la similitud sugiere que, en determinados escenarios, puede ser preferible utilizar k-NN, en lugar de los algoritmos de *ensemble*, que son mucho más lentos y demandantes tanto en el entrenamiento (i.e., requieren más datos para entrenar), como en la evaluación.

La implementación de los clasificadores de *ensemble*, y de CART, permite obtener el impacto que cada característica tiene en los resultados finales. Este dato evidencia que la característica más importante es *pressingTime*, con un peso de entre el 28 % y el 50 %, lo que concuerda con los resultados obtenidos por trabajos previos en ordenadores y teclados físicos. Nuestros resultados, sin embargo, contrastan con los de la literatura en cuanto al algoritmo SVM. Pese a ser uno de los más utilizados, normalmente con buenos resultados en el ámbito de las pantallas táctiles, en nuestro caso ninguna de las métricas obtiene un resultado aceptable, al menos con las características que hemos utilizado.

Aunque los resultados obtenidos en nuestro estudio por los diferentes algoritmos son algo peores que los mostrados en la literatura, son resultados aplicables a cada pulsación. Es decir, con una sola pulsación se puede obtener una predicción de la identidad del usuario con esas características. Si las acciones de control de acceso se tomasen combinando el resultado de varias pulsaciones (i.e., evaluando varias pulsaciones, y obteniendo un consenso), estas métricas mejorarían considerablemente. Para ello, en el trabajo se propone utilizar un mecanismo de votación entre distintos algoritmos antes de tomar la decisión sobre la identidad del usuario. Esta técnica denominada como *stacking* o *ensemble*, se traduciría, por ejemplo, en bloquear o no bloquear el dispositivo si tras varias predicciones se

tiene una percepción, lo suficientemente confiable, de que el usuario legítimo está siendo suplantado.

Teniendo esto en cuenta, y con los resultados obtenidos, cualquiera de los tres algoritmos con mejores resultados (i.e., GBC, ETC y k-NN) podría dotar de adaptatividad al sistema propuesto en el segundo artículo (ver Capítulo 3). Por ejemplo, haciendo que se borre del dispositivo la clave precompartida en el caso de detectarse una suplantación en la identidad del operador, o enviando una alerta a un sistema de monitorización para disparar mecanismos organizativos de respuesta.

Capítulo 6

Conclusiones y trabajos futuros

Esta tesis persigue, mediante un compendio de tres artículos de investigación, estudiar la autenticación continua, concretar su principios y propiedades, y definir sus aplicaciones en la defensa en profundidad de los sistemas de control de accesos. Los principios de la autenticación continua que hemos sintetizado son aplicables, y, de hecho, pueden redundar positivamente, en múltiples casos de uso, como el propuesto en el segundo artículo; pero sólo se puede conseguir un sistema de autenticación continua completo, que garantice el control de accesos adaptativo, y dé respuesta a todos estos principios, a través de la biometría conductual. Los resultados muestran la existencia de una gran cantidad de elementos que permiten la autenticación continua de las entidades participantes en un sistema de información, y cómo el estado del arte del aprendizaje automatizado cuenta con algoritmos que dan soporte a los diferentes requisitos que pueda tener un sistema de control de accesos, tanto de precisión, como de eficiencia.

6.1 Conclusión

El primer artículo, "*Access Control beyond Authentication*", recoge el estado del arte siguiendo un procedimiento sistemático. Seguir este enfoque sistemático ha permitido evitar sesgos, derivados principalmente del empleo del término "autenticación continua" para referirse a sistemas que, en muchas ocasiones, son meros sistemas dinámicos. También permite obtener una imagen del rendimiento actual de la autenticación continua con rigor, y evitando mensajes comerciales de la industria, involucrada en el desarrollo de productos que utilizan patrones conductuales, como los EDR. Se han sintetizado las características que debe tener un sistema de autenticación continua, y gracias a este estudio hemos podido conocer las diferentes entidades que pueden ser controladas mediante esta tecnología, mostrando que es aplicable a las interacciones entre diferentes dispositivos, y no es sólo válida para autenticar operadores humanos. Uno de los aspectos más críticos es la elección de características de la interacción, que pueden ofrecer un patrón conductual lo suficientemente bueno como para elevarlo a la categoría de biometría, siempre y cuando

se procese adecuadamente. Por ello, la enumeración de las diferentes aproximaciones para procesar los datos recogidos, presentes en el estado del arte, junto con sus rendimientos, ayuda a sentar las bases con las que trabajar en el futuro. Pese a que es una línea de investigación prolífica, en este estudio se han identificado las investigaciones con mayor impacto, que vertebran la evolución del estado del arte.

En el segundo artículo, "*C-Lock: Local Network Resilient Port Knocking System Based on TOTP*", mostramos un protocolo de autorización dinámico, basado en los principios de la autenticación continua. El protocolo, diseñado como un *port-knocking* cuya secuencia de golpeo se genera dinámicamente, contribuye a la seguridad de los sistemas de información, especialmente aquellos que se encuentran en una red local, o en cualquier otro ámbito en el que un adversario pueda tener acceso al contenido de las comunicaciones de red. Este problema (i.e., el de un adversario con acceso a información crítica para la seguridad del control de accesos) es exáctamente el mismo que enfrenta la autenticación continua, donde, si un adversario conoce, por ejemplo, las credenciales de acceso, no debería poder abrir o utilizar una sesión de trabajo; y sería rechazado si su perfil conductual no cuadra con el del operador legítimo. En este caso, en lugar de credenciales, el elemento secreto sería la secuencia de golpeo; pero al generarse de forma dinámica, la secuencia puede transmitirse sin que suponga un riesgo, incluso a través de un canal abierto. Buscando la defensa en profundidad del control de accesos, esta medida podría robustecer la comunicación entre un terminal y un servidor, pero su efectividad sigue reposando sobre la asunción de que la comunicación entre el operador, y el dispositivo de generación de códigos, no es quebrantada en ningún momento. Esta es una de las grandes carencias que tienen los sistemas dinámicos con respecto a la autenticación continua: siguen dependiendo de un elemento secreto, o especial, como único punto de fallo. Mediante la implantación de autenticación continua en el terminal móvil que genera los códigos, como otra defensa adicional, tendremos más garantías de que todo el canal de comunicación entre el operador y el servidor es seguro.

El tercer artículo, "*Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics*", desarrolla un análisis experimental con 7 algoritmos no supervisados de clasificación, entrenados con datos de tecleo de 100 participantes, extraídos del estudio HMOG [41]. Es el primer estudio en el que se evalúan todos estos algoritmos con un mismo conjunto de datos, y los resultados muestran cuáles de ellos pueden ser más beneficiosos en determinados casos de uso. El hallazgo más evidente es que el algoritmo GBC obtiene el mejor rendimiento en todas las métricas evaluadas, destacando en el *recall*, una métrica indispensable para cumplir con los requisitos de un sistema de autenticación continua. Pero otros algoritmos, que quizá ofrecen peores resultados, como k-NN, también son válidos para la autenticación continua, y pueden ser útiles en escenarios que requieran un menor coste computacional, o cuente con menos datos para el entrenamiento [58]. Los algoritmos GBC, RFC o k-NN podrían utilizarse para desarrollar un sistema de autenticación continua que protegiese de suplantaciones,

por ejemplo, el dispositivo en el que se generan los código del artículo 2 (ver 3). Además, en contraste con otras investigaciones del estado del arte, los resultados del algoritmo SVM arrojados por nuestro estudio lo descartan para la autenticación continua de los patrones de tecleo, al menos con las características que hemos utilizado. Particularmente, un hallazgo relevante arrojado por nuestra investigación, es la detección de qué características tienen más impacto en la autenticación continua mediante patrones de tecleo, otorgándole casi todo el protagonismo al tiempo de pulsación de tecla (i.e., *pressingTime*). Este artículo ofrece, finalmente, una base de conocimiento que puede ser utilizada para lo toma de decisiones, siempre que sea necesario implementar autenticación continua para proteger un sistema.

6.2 Trabajos futuros

Tras exponer las conclusiones de esta tesis, detectamos cuestiones que quedan abiertas, y que pueden abrir nuevas líneas de investigación. Los siguientes aspectos pueden ayudar a desarrollar nuevas contribuciones:

- La principal debilidad del método presentado en el segundo artículo (ver 3) es la posibilidad de que el operador del dispositivo sea suplantado. Sin embargo, si la generación de los códigos de golpeo pudiese basarse en parámetros conductuales, esta debilidad quedaría mitigada. Utilizando modelos de regresión, en lugar de los de clasificación, podrían generarse códigos de biometría conductual útiles para validar identidades.
- El desarrollo de mecanismos de combinación de veredictos, o de votación, puede mejorar considerablemente los resultados expuestos en el tercer artículo (ver 4). Otra línea de investigación que podría generar contribuciones al estado del arte es el estudio de qué técnicas de *stacking* ofrecerían mejores rendimientos.
- Aunque el tercer artículo desarrolla un caso de uso para teléfonos móviles, lo cierto es que tanto el entrenamiento como la evaluación se ha desarrollado en un entorno de laboratorio. Estos dispositivos tienen particularidades, computacionales, y energéticas, que requieren ser tratadas antes de implantar una solución. Es necesario evaluar qué modelos pueden implementarse en un dispositivo con estas características, y cuáles deben ser evaluados fuera. En el caso de que los datos deban ser tratados en un servidor, es necesario autenticar tanto el canal como el sistema emisor, o puede darse el caso de que estos datos se falsifiquen en el propio activo protegido. Además, en cualquiera de los dos escenarios, es imprescindible evaluar los riesgos para los datos de carácter personal, y la privacidad.
- En el caso de los modelos generados en el dispositivo móvil, todos los algoritmos abordados en nuestro estudio requieren del uso de datos de otros participantes. Se

debe abordar el uso de algoritmos de aprendizaje que permitan este entrenamiento sin poner en riesgo la privacidad, o incluso (y esta línea podría tener otras aplicaciones), mecanismos de generación de datos sintéticos que puedan ser utilizados para entrenar.

- Por último, aunque quizá sea la línea de investigación más relevante, se deben desarrollar modelos que permitan trabajar con los datos en sistemas distribuidos, como servidores, sin que suponga un riesgo adicional para la privacidad. El almacenamiento de los datos, de forma que un adversario, de cualquier tipo (e.g., incluido un administrador "curioso"), no tenga acceso a ellos más que para generar y evaluar modelos de autenticación continua, es un aspecto crítico para que se puedan desplegar este tipo de soluciones a gran escala. Aunque el estudio de tecnologías PET (i.e., *Privacy Enhacing Technologies*) está en auge, las aproximaciones para su implementación en la autenticación continua, como la propuesta de Wei et al. [59], siguen sin resolver el problema de la privacidad con éxito [60], o tiene unos costes computacionales inasumibles.

Bibliografía

[1] J. Junquera-Sánchez, "Técnicas avanzadas de descubrimiento y análisis de la red Tor", Trabajo de Fin de Grado, Universidad de Alcalá, 2018.

[2] S. Kumar y C. Zahn, "Mobile communications: Evolution and impact on business operations", *Technovation*, vol. 23, n.º 6, págs. 515-520, 1 de jun. de 2003, ISSN: 0166-4972. DOI: 10.1016/S0166-4972(02)00120-7. dirección: https://www.sciencedirect.com/science/article/pii/S0166497202001207 (visitado 19-11-2022).

[3] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd edition. Tokyo, New York: Wiley, 14 de abr. de 2008, 1088 págs., ISBN: 978-0-470-06852-6.

[4] D. Gollmann, "Access control", en *Computer Security*, Google-Books-ID: KTYxTfyjiOQC, John Wiley & Sons, 28 de feb. de 2011, pág. 65, ISBN: 978-0-470-74115-3.

[5] S. Rose, O. Borchert, S. Mitchell y S. Connelly, "Zero trust architecture", National Institute of Standards y Technology, 11 de ago. de 2020. DOI: 10.6028/NIST.SP.800-207. dirección: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (visitado 05-12-2020).

[6] O. N. de Seguridad. Autoridad Delegada para la Seguridad de la Información Clasificada, "Normas de la autoridad nacional para la protección de la información clasificada", Ministerio de Defensa, 2019, pág. 296. dirección: https://cpage.mpr.gob.es/producto/normas-de-la-autoridad-nacional-para-la-proteccion-de-la-informacion-clasificada-8/ (visitado 17-10-2022).

[7] M. T. Rahman, M. S. Rahman, H. Wang et al., "Defense-in-depth: A recipe for logic locking to prevail", *Integration*, vol. 72, págs. 39-57, 1 de mayo de 2020, ISSN: 0167-9260. DOI: 10.1016/j.vlsi.2019.12.007. dirección: https://www.sciencedirect.com/science/article/pii/S0167926019303694 (visitado 03-11-2022).

[8] J. R. Nirmal, R. B. Kiran y V. Hemamalini, "Improvised multi-factor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics", *Materials Today: Proceedings*, International Conference on Innovative Technology for Sustainable Development, vol. 62, págs. 4837-4843, 1 de ene. de 2022, ISSN: 2214-7853. DOI: 10.1016/j.matpr.2022.03.439. dirección: https://www.sciencedirect.com/science/article/pii/S2214785322017898 (visitado 03-11-2022).

[9] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity, version 1.1", National Institute of Standards y Technology, Gaithersburg, MD, NIST CSWP 04162018, 16 de abr. de 2018, NIST CSWP 04162018. DOI: 10.6028/NIST.CSWP.04162018. dirección: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (visitado 29-09-2022).

[10] Ministerio de Asuntos Económicos y Transformación Digital, *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*, 4 de mayo de 2022. dirección: https://www.boe.es/eli/es/rd/2022/05/03/311 (visitado 29-09-2022).

[11] D. Spence, G. Gross, C. d. Laat et al., "AAA Authorization Framework", Internet Engineering Task Force, Request for Comments RFC 2904, ago. de 2000, Num Pages: 35. DOI: 10.17487/RFC2904. dirección: https://datatracker.ietf.org/doc/rfc2904 (visitado 29-09-2022).

[12] E. Parliament, *Regulation (EU) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC*, Legislative Body: EP, CONSIL, 23 de jul. de 2014. dirección: http://data.europa.eu/eli/reg/2014/910/oj/eng (visitado 29-09-2022).

[13] I. Velásquez, A. Caro y A. Rodríguez, "Authentication schemes and methods: A systematic literature review", *Information and Software Technology*, vol. 94, págs. 30-37, 1 de feb. de 2018, ISSN: 0950-5849. DOI: 10.1016/j.infsof.2017.09.012. dirección: https://www.sciencedirect.com/science/article/pii/S0950584916301501 (visitado 29-09-2022).

[14] R. Fagin, "On an authorization mechanism", *ACM Transactions on Database Systems*, vol. 3, n.º 3, págs. 310-319, sep. de 1978, ISSN: 0362-5915, 1557-4644. DOI: 10.1145/320263.320288. dirección: https://dl.acm.org/doi/10.1145/320263.320288 (visitado 29-09-2022).

[15] X. Jin, R. Krishnan y R. Sandhu, "A unified attribute-based access control model covering DAC, MAC and RBAC", en *Data and Applications Security and Privacy XXVI*, N. Cuppens-Boulahia, F. Cuppens y J. Garcia-Alfaro, eds., ép. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2012, págs. 41-55, ISBN: 978-3-642-31540-4. DOI: 10.1007/978-3-642-31540-4_4.

[16] N. Papatheodoulou y N. Sklavos, "Architecture & system design of Authentication, Authorization, & Accounting services", en *IEEE EUROCON 2009*, mayo de 2009, págs. 1831-1837. DOI: 10.1109/EURCON.2009.5167894.

[17] P. Arias-Cabarcos, C. Krupitzer y C. Becker, "A Survey on Adaptive Authentication", *ACM Computing Surveys*, vol. 52, n.º 4, 80:1-80:30, 11 de sep. de 2019, ISSN: 0360-0300. DOI: 10.1145/3336117. dirección: https://doi.org/10.1145/3336117 (visitado 29-09-2022).

[18] L. Mecke, K. Pfeuffer, S. Prange y F. Alt, "Open Sesame! User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors", en *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*, ép. MUM 2018, New York, NY, USA: Association for Computing Machinery, 25 de nov. de 2018, págs. 153-159, ISBN: 978-1-4503-6594-9. DOI: 10.1145/3282894.3282923. dirección: https://doi.org/10.1145/3282894.3282923 (visitado 28-09-2022).

[19] V. M. Patel, R. Chellappa, D. Chandra y B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges", *IEEE Signal Processing Magazine*, vol. 33, n.º 4, págs. 49-61, jul. de 2016, Conference Name: IEEE Signal Processing Magazine, ISSN: 1558-0792. DOI: 10.1109/MSP.2016.2555335.

[20] D. Bradbury, "Okta's investigation of the january 2022 compromise". dirección: https://www.okta.com/blog/2022/03/oktas-investigation-of-the-january-2022-compromise/ (visitado 09-08-2022).

[21] C. Hale, "Security in Depth". dirección: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/security-in-depth (visitado 20-08-2022).

[22] M. Calvo y M. Beltrán, "A model for risk-based adaptive security controls", *Computers & Security*, vol. 115, pág. 102 612, 1 de abr. de 2022, ISSN: 0167-4048. DOI: 10.1016/j.cose.2022.102612. dirección: https://www.sciencedirect.com/science/article/pii/S0167404822000116 (visitado 20-08-2022).

[23] S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics", págs. 111-114, 1 de ene. de 1995, Publisher: IET Digital Library. DOI: 10.1049/cp:19950480. dirección: https://digital-library.theiet.org/content/conferences/10.1049/cp_19950480 (visitado 05-12-2020).

[24] INCIBE-CERT, *Tecnologías biométricas aplicadas a la ciberseguridad*. dirección: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf (visitado 10-08-2022).

[25] B. Hassan, E. Izquierdo y T. Piatrik, "Soft biometrics: A survey", *Multimedia Tools and Applications*, 2 de mar. de 2021, ISSN: 1573-7721. DOI: 10.1007/s11042-021-10622-8. dirección: https://doi.org/10.1007/s11042-021-10622-8 (visitado 16-08-2022).

[26] A. Dantcheva, C. Velardo, A. D'Angelo y J.-L. Dugelay, "Bag of soft biometrics for person identification", *Multimedia Tools and Applications*, vol. 51, n.º 2, págs. 739-777, 1 de ene. de 2011, ISSN: 1573-7721. DOI: 10.1007/s11042-010-0635-7. dirección: https://doi.org/10.1007/s11042-010-0635-7 (visitado 16-08-2022).

[27] P. Phillips, A. Martin, C. Wilson y M. Przybocki, "An introduction evaluating biometric systems", *Computer*, vol. 33, n.º 2, págs. 56-63, feb. de 2000, Conference Name: Computer, ISSN: 1558-0814. DOI: 10.1109/2.820040.

[28] A. K. Jain, "Biometric recognition: Overview and recent advances", en *Progress in Pattern Recognition, Image Analysis and Applications*, L. Rueda, D. Mery y J. Kittler, eds., ép. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2007, págs. 13-19, ISBN: 978-3-540-76725-1. DOI: 10.1007/978-3-540-76725-1_2.

[29] S. Eberz, K. B. Rasmussen, V. Lenders e I. Martinovic, "Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics", en *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ép. ASIA CCS '17, New York, NY, USA: Association for Computing Machinery, 2 de abr. de 2017, págs. 386-399, ISBN: 978-1-4503-4944-4. DOI: 10.1145/3052973.3053032. dirección: https://doi.org/10.1145/3052973.3053032 (visitado 16-08-2022).

[30] M. Sivaram, M. U. Ahamed A, D. Yuvaraj, G. Megala, V. Porkodi y M. Kandasamy, "Biometric Security and Performance Metrics: FAR, FER, CER, FRR", en *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, dic. de 2019, págs. 770-772. DOI: 10.1109/ICCIKE47802.2019.9004275.

[31] J. V. Kulkarni, B. D. Patil y R. S. Holambe, "Orientation feature for fingerprint matching", *Pattern Recognition*, vol. 39, n.º 8, págs. 1551-1554, 1 de ago. de 2006, ISSN: 0031-3203. DOI: 10.1016/j.patcog.2006.03.007. dirección: https://www.sciencedirect.com/science/article/pii/S0031320306001208 (visitado 29-09-2022).

[32] R. Bolle, S. Pankanti y N. Ratha, "Evaluation techniques for biometrics-based authentication systems (FRR)", en *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, ISSN: 1051-4651, vol. 2, sep. de 2000, 831-837 vol.2. DOI: 10.1109/ICPR.2000.906204.

[33] A. A. E. Ahmed e I. Traore, "A New Biometric Technology Based on Mouse Dynamics", *IEEE Transactions on Dependable and Secure Computing*, vol. 4, n.º 3, págs. 165-179, jul. de 2007, Conference Name: IEEE Transactions on Dependable and Secure Computing, ISSN: 1941-0018. DOI: 10.1109/TDSC.2007.70207.

[34] K. Dharavath, F. A. Talukdar y R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review", en *2013 IEEE International Conference on Computational Intelligence and Computing Research*, dic. de 2013, págs. 1-7. DOI: 10.1109/ICCIC.2013.6724278.

[35] P.-W. Tsai, M. K. Khan, J.-S. Pan y B.-Y. Liao, "Interactive Artificial Bee Colony Supported Passive Continuous Authentication System", *IEEE Systems Journal*, vol. 8, n.º 2, págs. 395-405, jun. de 2014, Conference Name: IEEE Systems Journal, ISSN: 1937-9234. DOI: 10.1109/JSYST.2012.2208153.

[36] S. Eberz, K. B. Rasmussen, V. Lenders e I. Martinovic, "Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics", *ACM Transactions on Privacy and Security*, vol. 19, n.º 1, 1:1-1:31, 16 de jun. de 2016, ISSN: 2471-2566. DOI: 10.1145/2904018. dirección: https://doi.org/10.1145/2904018 (visitado 29-09-2022).

[37] G. Ryu, S. Park, D. Choi et al., "Active Authentication Experiments Using Actual Application Usage Log", en *Proceedings of the First Workshop on Radical and Experiential Security*, ép. RESEC '18, New York, NY, USA: Association for Computing Machinery, 24 de mayo de 2018, págs. 9-16, ISBN: 978-1-4503-5757-9. DOI: 10.1145/3203422.3203424. dirección: https://doi.org/10.1145/3203422.3203424 (visitado 29-09-2022).

[38] H. A. Shabeer y P. Suganthi, "Mobile Phones Security Using Biometrics", en *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, vol. 4, dic. de 2007, págs. 270-274. DOI: 10.1109/ICCIMA.2007.182.

[39] K. W. Miller, J. Voas y G. F. Hurlburt, "BYOD: Security and Privacy Considerations", *IT Professional*, vol. 14, n.º 5, págs. 53-55, sep. de 2012, Conference Name: IT Professional, ISSN: 1941-045X. DOI: 10.1109/MITP.2012.93.

[40] M. Frank, R. Biedert, E. Ma, I. Martinovic y D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication", *IEEE Transactions on Information Forensics and Security*, vol. 8, n.º 1, págs. 136-148, ene. de 2013, Conference Name: IEEE Transactions on Information Forensics and Security, ISSN: 1556-6021. DOI: 10.1109/TIFS.2012.2225048.

[41] Z. Sitová, J. Šeděnka, Q. Yang et al., "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users", *IEEE Transactions on Information Forensics and Security*, vol. 11, n.º 5, págs. 877-892, mayo de 2016, Conference Name: IEEE Transactions on Information Forensics and Security, ISSN: 1556-6021. DOI: 10.1109/TIFS.2015.2506542.

[42] M. Guennoun, N. Abbad, J. Talom, S. M. M. Rahman y K. El-Khatib, "Continuous authentication by electrocardiogram data", en *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH)*, sep. de 2009, págs. 40-42. DOI: 10.1109/TIC-STH.2009.5444466.

[43] M. Shozawa, R. Yokote, S. Hidano, C.-H. Wu e Y. Matsuyama, "Brain signal based continuous authentication: Functional NIRS approach", en *Advances in Computational Intelligence*, I. Rojas, G. Joya y J. Cabestany, eds., ép. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2013, págs. 171-180, ISBN: 978-3-642-38682-4. DOI: 10.1007/978-3-642-38682-4_20.

[44] J. Wang, M. Ni, F. Wu, S. Liu, J. Qin y R. Zhu, "Electromagnetic radiation based continuous authentication in edge computing enabled internet of things", *Journal of Systems Architecture*, vol. 96, págs. 53-61, 1 de jun. de 2019, ISSN: 1383-7621. DOI: 10.1016/j.sysarc.2018.12.003. dirección: https://www.sciencedirect.com/science/article/pii/S1383762118304491 (visitado 11-08-2022).

[45] C. Bekara, "Security issues and challenges for the IoT-based smart grid", *Procedia Computer Science*, The 9th International Conference on Future Networks and Communications (FNC'14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC'14)/Affiliated Workshops, vol. 34, págs. 532-537, 1 de ene. de 2014, ISSN: 1877-0509. DOI: 10.1016/j.procs.2014.07.064. dirección: https://www.sciencedirect.com/science/article/pii/S1877050914009193 (visitado 11-08-2022).

[46] F. H. Al-Naji y R. Zagrouba, "A survey on continuous authentication methods in internet of things environment", *Computer Communications*, vol. 163, págs. 109-133, 1 de nov. de 2020, ISSN: 0140-3664. DOI: 10.1016/j.comcom.2020.09.006. dirección: https://www.sciencedirect.com/science/article/pii/S0140366420319204 (visitado 29-09-2022).

[47] J. Liu, F. R. Yu, C.-H. Lung y H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks", *IEEE Transactions on Wireless Communications*, vol. 8, n.º 2, págs. 806-815, feb. de 2009, Conference Name: IEEE Transactions on Wireless Communications, ISSN: 1558-2248. DOI: 10.1109/TWC.2009.071036.

[48] J. Junquera-Sánchez, C. Cilleruelo-Rodríguez, L. de-Marcos y J. J. Martínez-Herráiz, "JBCA: Designing an adaptative continuous authentication architecture", en *Advances in Physical Agents II*, L. M. Bergasa, M. Ocaña, R. Barea, E. López-Guillén y P. Revenga, eds., ép. Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2021, págs. 194-209, ISBN: 978-3-030-62579-5. DOI: 10.1007/978-3-030-62579-5_14.

[49] L. de-Marcos, C. Cilleruelo, J. Junquera-Sánchez y J.-J. Martínez-Herráiz, "A framework for BYOD continuous authentication: Case study with soft-keyboard metrics for healthcare environment", en *Applied Informatics*, H. Florez y S. Misra, eds., ép. Communications in Computer and Information Science, Cham: Springer International Publishing, 2020, págs. 347-358, ISBN: 978-3-030-61702-8. DOI: 10.1007/978-3-030-61702-8_24.

[50] E. Klieme, J. Wilke, N. van Dornick y C. Meinel, "FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication", en *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, ISSN: 2324-9013, dic. de 2020, págs. 1857-1867. DOI: 10.1109/TrustCom50675.2020.00254.

[51] L. Hernández-Álvarez, J. M. de Fuentes, L. González-Manzano y L. Hernández Encinas, "Privacy-preserving sensor-based continuous authentication and user profiling: A review", *Sensors*, vol. 21, n.º 1, pág. 92, ene. de 2021, Number: 1 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1424-8220. DOI: 10.3390/s21010092. dirección: https://www.mdpi.com/1424-8220/21/1/92 (visitado 29-09-2022).

[52] A. F. Baig y S. Eskeland, "Security, privacy, and usability in continuous authentication: A survey", *Sensors*, vol. 21, n.º 17, pág. 5967, ene. de 2021, Number: 17 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1424-8220. DOI: 10.3390/s21175967. dirección: https://www.mdpi.com/1424-8220/21/17/5967 (visitado 29-09-2022).

[53] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez y C. Busch, *An Overview of Privacy-enhancing Technologies in Biometric Recognition*, 21 de jun. de 2022. DOI: 10.48550/arXiv.2206.10465. arXiv: 2206.10465[cs]. dirección: http://arxiv.org/abs/2206.10465 (visitado 20-08-2022).

[54] S. Chirita. "Enhancing next-generation security with continuous authentication: XDR explained", TypingDNA Blog. (24 de feb. de 2022), dirección: https://blog.typingdna.com/enhancing-next-generation-security-with-continuous-authentication-xdr-explained/ (visitado 05-10-2022).

[55] M. E. Schuckers, "Receiver operating characteristic curve and equal error rate", en *Computational Methods in Biometric Authentication: Statistical Methods for Performance Evaluation*, ép. Information Science and Statistics, M. E. Schuckers, ed., London: Springer, 2010, págs. 155-204, ISBN: 978-1-84996-202-5. DOI: 10.1007/978-1-84996-202-5_5. dirección: https://doi.org/10.1007/978-1-84996-202-5_5 (visitado 07-11-2022).

[56] T. Hastie, R. Tibshirani y J. Friedman, *The Elements of Statistical Learning* (Springer Series in Statistics). New York, NY: Springer, 2009, ISBN: 978-0-387-84857-0 978-0-387-84858-7. DOI: 10.1007/978-0-387-84858-7. dirección: http://link.springer.com/10.1007/978-0-387-84858-7 (visitado 07-11-2022).

[57] F. Pedregosa, G. Varoquaux, A. Gramfort et al., "Scikit-learn: Machine Learning in Python", *Journal of Machine Learning Research*, vol. 12, págs. 2825-2830, 2011.

[58] T.-S. Lim, W.-Y. Loh e Y.-S. Shih, "A comparison of prediction accuracy, complexity, and training time of thirty-three old and new classification algorithms", *Machine Learning*, vol. 40, n.º 3, págs. 203-228, 1 de sep. de 2000, ISSN: 1573-0565. DOI: 10.1023/A:1007608224229. dirección: https://doi.org/10.1023/A:1007608224229 (visitado 20-11-2022).

[59] F. Wei, P. Vijayakumar, N. Kumar, R. Zhang y Q. Cheng, "Privacy-Preserving Implicit Authentication Protocol Using Cosine Similarity for Internet of Things", *IEEE Internet of Things Journal*, vol. 8, n.º 7, págs. 5599-5606, abr. de 2021, Conference Name: IEEE Internet of Things Journal, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3031486.

[60] S. Eskeland y A. F. Baig, *Cryptanalysis of a privacy-preserving behavior-oriented authentication scheme*, Report Number: 1589, 2022. dirección: https://eprint.iacr.org/2022/1589 (visitado 20-11-2022).