CAPÍTULO 6. CONCLUSIONES

En este capítulo, en primer lugar, se exponen las conclusiones generales extraídas tras la realización de esta tesis doctoral. En segundo lugar, se exponen las conclusiones específicas asociadas a cada uno de los objetivos que se detallaron en el primer capítulo. En tercer lugar, se presentan las posibles líneas de investigación futura que han surgido. Finalmente, se detallan las principales contribuciones y publicaciones científicas que han derivado de la elaboración de la presente tesis.

6.1. Conclusiones generales

El presente trabajo de tesis doctoral tiene fijados dos objetivos generales para validar la hipótesis de partida. El primer objetivo se centra en el diseño de un flujo de trabajo que permita la integración de los métodos análisis de comportamiento en los principales estándares de gestión de identidades federada. Este objetivo se alcanzó en el Capítulo 3 del presente documento. Por otro lado, el segundo objetivo se centra en el diseño de un método de análisis de comportamiento capaz de combinar información de múltiples fuentes de datos. Este objetivo también se ha podido alcanzar en el Capítulo 4 del presente documento. Cabe destacar, que la metodología fijada al comienzo de este documento ha sido fundamental y determinante en la consecución de dichos objetivos.

Por lo expuesto anteriormente, la principal conclusión del presente trabajo de tesis doctoral, puesto que los dos objetivos generales se han podido alcanzar, es que la hipótesis de partida ha quedado demostrada. Esto significa, por lo tanto, que es posible mejorar los niveles de seguridad proporcionados por los estándares de gestión de identidades federados utilizando para ello técnicas de análisis de comportamiento de los usuarios. Y además, que es posible mejorar la eficacia de los modelos de análisis de comportamiento del estado del arte utilizando técnicas de combinación de la información.

6.2. Conclusiones específicas

6.2.1. Conclusiones del flujo de trabajo

Las principales conclusiones extraídas en relación con el flujo de trabajo propuesto se pueden resumir en:

- El flujo de trabajo propuesto aumenta los niveles de seguridad de los estándares actuales que siguen el modelo federado (en relación con los

ataques de suplantación de identidad) y puede ser fácilmente implementado por cualquier RP siguiendo las directrices proporcionadas.

- La elección de los atributos que las RPs han de emplear para generar una huella digital dependerá, en gran medida, del propio dominio y caso de uso particular. Sin embargo, los perfiles de seguridad propuestos son una referencia útil como punto de partida.

- Las RPs deben tener un equilibrio entre eficacia y usabilidad ya que la introducción de técnicas de análisis de comportamiento en algunos casos de uso puede añadir latencias significativas a los flujos de identificación y autenticación tradicionales.

- El flujo de trabajo propuesto es un claro ejemplo de caso de uso en el que se aumentan los riesgos para la privacidad con el objetivo de mitigar los riesgos para la seguridad. Existen multitud de dominios en los que los usuarios seguramente estén dispuestos a asumir este coste, pero otros, considerados "banales" en los que probablemente no sea así. Por lo tanto las RPs deben informar del tratamiento de datos que van a realizar (siguiendo la regulación vigente y el principio de responsabilidad proactiva), así como de la información que van a recopilar para generar la huella digital. Es el usuario final el que debe proporcionar su consentimiento explícito e informado, debe tener siempre el poder para decidir si quiere que se le apliquen o no este tipo de mecanismos de análisis de comportamiento.

- La integración del flujo de trabajo propuesto en los flujos actuales de identificación y autenticación puede llevarse a cabo utilizando los propios mecanismos especificados en los estándares actuales. Esto implica que la integración puede realizarse en las etapas de implementación y, por lo tanto, es relativamente sencilla de realizar ya que no exige ningún cambio o modificación en las especificaciones vigentes (y que ya están ampliamente extendidas en entornos de producción).

6.2.2. Conclusiones del método de combinación de información de comportamientos

Las principales conclusiones relacionadas con este objetivo de la investigación realizada se pueden resumir en:

- Los RTE han demostrado ser una técnica prometedora para representar información de comportamientos. Esto se debe a que la discretización de la información se logra con una pérdida de información mínima.

- La representación de la información de comportamientos en forma de secuencia de caracteres o símbolos permite realizar la combinación de información a nivel de características de forma efectiva.

- El uso de técnicas de alineamiento de ADN permite comparar de forma precisa dinámicas de comportamiento, lo que repercute de forma directa en la eficacia de los métodos de detección de anomalías de comportamiento.

- El uso de técnicas de *clustering* basadas en densidades permite acotar la información utilizada para entrenar los modelos de análisis de comportamientos y para su posterior fase de predicción. Esto consigue una reducción en las latencias añadidas a los flujos de identificación y autenticación que integren el método propuesto.

- El modelo basado en riesgos permite detectar anomalías de comportamiento a lo largo del tiempo. Este modelo puede adaptarse acorde a los requisitos de los usuarios para ser más permisivo o restrictivo dependiendo del dominio de aplicación y del caso de uso.

- El método propuesto es más eficaz detectando anomalías de comportamiento que otras propuestas específicas encontradas en la literatura y que otros algoritmos del estado del arte como RF y SVM. Esto se ha demostrado al evaluarlo sobre los conjuntos de datos de UEBA y TWOS. En el caso del conjunto de datos de TWOS, el método propuesto siempre obtiene EER menores para todas las casuísticas de evaluación. Estas mejoras van desde el 48,5 % hasta el 1,6 % dependiendo del algoritmo o método comparado y las fuentes de información consideradas.

6.3. Líneas de investigación futuras

La elaboración de esta tesis doctoral ha permitido identificar un conjunto de líneas de investigación que en el futuro pueden complementar, mejorar o extender este trabajo de investigación. Estas son las más interesantes o prometedoras:

- Las técnicas de análisis de comportamientos pueden ser integradas e implementadas dentro de un estándar federado, no solo en la parte que concierne a la RP (como se ha expuesto en esta tesis), sino en la parte del IdP. De esta forma, existen multitud de casos de uso como:

    1. Autenticación continua: el propio IdP puede utilizar la información de las peticiones de autenticación y/o autorización para generar un método de análisis de comportamiento de tal manera que, analizando datos históricos,

determine el riesgo en tiempo real de las interacciones que está realizando un usuario. De esta manera, el IdP puede anular, por ejemplo, la *cookie* de sesión si así lo sugiere el método de análisis de comportamientos.

2. Detección de suplantación o fraude: el IdP puede utilizar el histórico de interacciones del usuario para determinar, a posteriori, si se ha producido una suplantación de identidad o fraude. La gran ventaja de los modelos de análisis de comportamientos que se utilizarían con este objetivo es que al poder dejar de lado la eficiencia (no importa que la latencia sea alta porque no se ejecuta el modelo en tiempo real), se pueden generar modelos que primen la eficacia y, por lo tanto, detectar con mayor precisión las posibles brechas de seguridad.

3. Registro dinámico de dispositivos y usuarios: normalmente el registro de usuarios y dispositivos se realiza de forma manual y remota en el IdP. Sin embargo, hoy en día con el avance del IoT, existen multitud de sensores que se deben registrar en un IdP (fase de *enrollment* o de *on-boarding*). Los métodos de análisis de comportamientos pueden utilizarse para completar esta fase de registro de forma eficiente o automática teniendo en cuenta el comportamiento observado durante un periodo de tiempo, o incluso analizando el comportamiento de dispositivos vecinos o similares en conjunto.

- El método de combinación de información propuesto se basa en discretizar la información de comportamiento proveniente de múltiples fuentes de datos heterogéneas utilizando una técnica novedosa de SAX basada en el uso de RTEs. Esta técnica ha demostrado empíricamente ser efectiva para este propósito, sin embargo, el uso de técnicas de lógica difusa o NNs han demostrado ser bastante efectiva a la hora de generar *embeddings* en otros ámbitos. Es por esto que una línea de investigación futura es la evaluación de estos tipos de algoritmos, en cuanto a eficiencia y eficacia, en el ámbito del análisis de comportamientos.

- La comparación de secuencias de caracteres o símbolos se realiza en esta tesis por medio de técnicas de alineamiento de secuencias de ADN. Sin embargo, hoy en día existen multitud de métricas de similitud entre este tipo de secuencias. Una posible línea de investigación futura sería evaluar otras métricas o incluso, realizar una combinación de matrices de similitud obtenidas utilizando diferentes métricas de forma independiente. Esto último se puede materializar mediante una combinación de *kernels* con el objetivo de ponderar las diferentes virtudes o fallos de cada una de ellas por separado.

- El método de combinación propuesto en esta tesis es escalable, es decir, se podrían considerar nuevas fuentes de información de forma sencilla.

Esto permite añadir nuevos datos a los modelos que permiten identificar las anomalías en el comportamiento de los usuarios y por lo tanto, potenciales brechas de seguridad. Sería conveniente evaluarlo en un entorno IoT, donde los recursos computacionales disponibles en los dispositivos son limitados. De este modo, para escalar el método y combinar más fuentes de información ser debería recurrir al *edge computing* para distribuir el procesamiento adicional requerido.

6.4. Principales contribuciones y publicaciones derivadas de la tesis

Las principales contribuciones del presente trabajo de tesis doctoral se resumen en:

1. Análisis en profundidad de los principales trabajos en el ámbito del análisis de comportamiento.

2. Flujo de trabajo para la integración de los modelos de análisis de comportamiento en los estándares de gestión de identidades federados.

3. Modelo de análisis de comportamiento que combina información recogida de fuentes de datos heterogéneas.

4. Nuevo conjunto de datos que contiene dinámicas de comportamiento de usuarios.

Las publicaciones realizadas durante el desarrollo de esta tesis doctoral en relación con estas contribuciones son las siguientes:

1. A. G. Martín, I. M. de Diego, A. Fernández-Isabel, M. Beltrán y Fernández, R. R. “Combining user behavioural information at the feature level to enhance continuous authentication systems” . Knowledge-Based Systems, 108544, 2022

2. A. G. Martín, M. Beltrán, A. Fernández-Isabel e I. M. de Diego, “An approach to detect user behaviour anomalies within identity federations” Computers & Security, vol. 108, p. 102 356, 2021.

3. A. G. Martín, A. Fernández-Isabel, I. M. de Diego y M. Beltrán, “A survey for user behavior analysis based on machine learning techniques: current models and applications,” Applied Intelligence, pp. 1-27, 2021.

4. A. G. Martín, M. Beltrán, A. Fernández-Isabel e I. M. de Diego, “Keystroke and Mouse Dynamics for UEBA Dataset”, Mendeley Data, v2, 2020

5. A. G. Martín, M. Beltrán, “Mejora de la seguridad de esquemas de gestión de identidades federados mediante técnicas de User Behaviour Analytics”, V Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2019), pp. 159-166,2019

Cada una de las publicaciones aquí presentadas se corresponden con un capítulo del presente trabajo de tesis doctoral y con una o varias contribuciones del mismo. De este modo, el Capítulo 1 se corresponde con la publicación [18]. En él se presentan los principales objetivos e ideas que surgieron al comienzo de la realización de la presente tesis. En la publicación [4] se aborda el estado del arte presentado en el Capítulo 2. Esta publicación se corresponde con la primera contribución. El Capítulo 3 se corresponde con la publicación [110] y en él se presentan la segunda y tercera contribución, es decir, el flujo de trabajo para lograr la integración en los estándares federados y el conjunto de datos que incluye dinámicas de comportamiento. El Capítulo 4 se corresponde con la publicación [130], y en él se presenta la cuarta contribución, es decir, el modelo de análisis de comportamiento que combina información. Finalmente, los experimentos abordados en el Capítulo 5, y las conclusiones obtenidas en el Capítulo 6 se ven reflejadas en todas estas publicaciones de forma simultánea.