13

RETRATO DE LAS PERSONALIDADES DIGITALES: IDENTIFICACIÓN DE VULNERABILIDADES DE PLURIDENTIDAD EN LA VIDA DIGITAL

Miguel Ángel Olivero
Antonia Bertolino
Francisco José Domínguez-Mayo
María José Escalona
Ilaria Matteucci

El creciente uso de Internet con fines sociales hace florecer los datos en línea disponibles sobre todos nosotros, y promueve el concepto de la Persona Digital. De hecho, la mayoría de nosotros estamos representados en la red por más de una identidad, lo que aquí definimos como una *Pluridentidad.* Esta tendencia genera grandes riesgos ya que la seguridad de una Persona Digital puede ser explotada si sus datos y su seguridad no se gestionan eficazmente. En este capítulo nos centramos específicamente en un nuevo tipo de ataque digital que se puede llevar a cabo al combinar piezas de datos pertenecientes a una misma Pluridentidad con el fin de retratar a su objetivo. Los detalles de algunas víctimas pueden ser de una precisión tal que, al analizar la información recopilada sobre una Pluridentidad, los atacantes pueden ejecutar ataques de ingeniería social muy personalizados, o incluso eludir los mecanismos de seguridad. Se han caracterizado estos ataques a la Pluridentidad como un problema de la seguridad en sistemas de sistemas virtuales, cuyos sistemas constituyentes son las identidades individuales, así como los propios seres humanos. Este capítulo describe una estrategia para identificar las vulnerabilidades causadas por la sobreexposición debido a la combinación de datos de las identidades

constituyentes de una Pluridentidad. Para este fin se describe el Metamodelo de Representación de Personas Digitales, y el proceso relacionado de Análisis de Representación de Personajes de Pluridentidad Digital que apoya la arquitectura de datos de diferentes identidades: dicho modelo y proceso se pueden utilizar para identificar las vulnerabilidades de una Pluridentidad debido a su explotación como Sistema de Sistemas. El enfoque ha sido validado sobre las pluridentidades de diecisiete candidatos seleccionados de una filtración de datos, recuperando los datos accesibles públicamente de su Personalidad Digital, y comparándolos con los mecanismos de seguridad de sus Pluridentities. Tras analizar los resultados de algunos de los temas analizados se pudieron detectar varias vulnerabilidades.

13.1 INTRODUCCIÓN

El concepto de Personalidad Digital se empezó a emplear a principios de los 90 [6] para denominar la parte digital de la identidad de un individuo. Hace más de dos décadas ese trabajo ya advertía de los riesgos inherentes de la gestión de las grandes cantidades de datos que mantienen las organizaciones ya sean empresariales o gubernamentales [6]. Hoy en día, el uso generalizado de Internet con fines sociales y laborales ha enriquecido y aumentado considerablemente los datos públicos disponibles sobre todos en la red y, por lo tanto, ha impulsado el concepto de la Personalidad Digital.

Hoy en día, internet se utiliza comúnmente para socializar y comunicarse por todo el mundo. Existen redes sociales para casi todos los temas imaginables. Las personas pueden compartir sus intereses y actividades empujados por la necesidad humana de visibilizar lo que les gusta o no les gusta. Las relaciones en las redes sociales se basan en la confianza, reputación y reciprocidad que se mantiene con otros usuarios.

Este fenómeno, por otro lado, hace que la Personalidad Digital esté continuamente en riesgo, ya que internet también es una fuente de nuevas oportunidades de ataques [13]. Hay una extensa lista de diferentes ataques digitales dependiendo del propósito del atacante y la posibilidad de éste de interactuar con la víctima [15] [1] [43].

Los datos que las personas publican pueden ser utilizados para analizar sus perfiles y estudiar su comportamiento para predecir sus próximas acciones [3] [29]. Por lo tanto, nuestros datos se han convertido en una oportunidad de oro para que los atacantes aprendan sobre nosotros, detecten usuarios incautos y diseñen ataques personalizados. Los atacantes necesitan identificar a sus potenciales víctimas, y las redes sociales son una herramienta que facilita la identificación de objetivos vulnerables.

Perfilar a las personas es una tendencia en ataques digitales recientes [4]: implica el uso de fragmentos de datos disponibles públicamente en Internet y combinarlos con otros para representar a una persona objetivo. Algunas de estas personas describen públicamente su Personalidad Digital con tanta precisión que los atacantes pueden ejecutar fácilmente ataques de ingeniería social atendiendo a las características individuales de su víctima [43], o incluso podrían eludir algunos mecanismos de seguridad sólo mediante el uso de la información recopilada. Estos ataques de perfilar víctimas han demostrado tener consecuencias de diferente impacto [41].

En este estudio, se resaltan las vulnerabilidades de nuestra Personalidad Digital, que pueden surgir a causa de lo que llamamos una Representación Digital de la Persona (RDP): con este término nos referimos al emparejamiento y la combinación imprevista de fuentes de datos relativas a otras identidades que se generan en diferentes contextos sociales (es decir, una pluridentidad),y que resultan en una sobreexposición de información que puede pasar por alto.

Estas vulnerabilidades emergentes existen debido a la combinación específica de varias identidades. Para gestionar esa configuración se aplica un enfoque empleando los Sistemas de Sistemas (SdS; en inglés: System of Systems, SoS) [9] [24]: consideramos cada identidad como un sistema constituyente, y la Pluridentidad como el propio SdS. En un SdS, a pesar de que cada sistema es lo suficientemente seguro por sí solo, la seguridad de un SdS puede verse comprometida mediante una combinación de los datos disponibles de los sistemas constituyentes. De este modo, las vulnerabilidades de un SdS sólo existen debido a un comportamiento emergente [27] que surge de una configuración que combina los recursos de los sistemas constituyentes.

Se propone una estrategia original para la evaluación de vulnerabilidades debido a RDP. Con este fin, primero introducimos modelos para estructurar y relacionar los datos de pluridentidades de la Personalidad Digital. A continuación, mostramos cómo estos modelos se pueden analizar para identificar posibles vulnerabilidades RDP.

Los modelos, métodos y técnicas desarrollados en nuestro enfoque han sido evaluados en diecisiete sujetos seleccionados a partir de una filtración de datos de un panel de encuestas en línea. A estas 17 personas, elegidas por poseer más identidades digitales, se les ha “retratado” su Personalidad Digital, recuperando y combinando los datos que expusieron públicamente en diferentes contextos. En esta evaluación, se ha tenido en cuenta la seguridad de aquellos sistemas en los que se encontró una identidad de la Persona Digital, para determinar el impacto de la sobreexposición frente a posibles ataques. Después de analizar los resultados y hacer coincidir la

información sobre las identidades de la Persona Digital, se detectaron algunas vulnerabilidades.

13.1.1 Motivación

En tecnologías de la información, se ha introducido el concepto de Sistema de Sistemas (SdS) [9] para denotar una arquitectura virtual distribuida y compuesta cuyos resultados se logran como la combinación de los resultados parciales de sus sistemas constituyentes. En un SdS, los sistemas constituyentes mantienen su autonomía y, en algunos casos, podrían incluso no ser conscientes de la misión global a la que pueden estar contribuyendo: simplemente ofrecen su servicio que, cuando participa con otros sistemas, permite alcanzar algunos objetivos globales que no podrían ser alcanzados por los sistemas individuales por sí solos.

Hoy en día, los Sistemas de Sistemas y la Ingeniería de Sistemas de Sistemas (IsdS; en inglés: System of Systems Engineering, SoSE) son vistos como una oportunidad para que la comunidad de ingeniería de sistemas defina sistemas complejos.

Aquí proponemos una perspectiva novedosa para tratar las identidades digitales, es decir, que los usuarios que tengan cuentas en diferentes sistemas puedan interpretarse como un SdS, cuyos sistemas constituyentes son las identidades de usuario individuales.

Desde la perspectiva de un SdS en el contexto de la Personalidad Digital, buscamos vectores de ataque, rutas o medios que podrían permitir a un atacante explotar las vulnerabilidades en el SdS. Los resultados colaborativos producidos después de combinar estos sistemas en un SdS se denominan comportamiento emergente (en inglés: Emergent Behavior). Tales comportamientos emergentes pueden incluir resultados esperados, así como resultados inesperados tales como vectores de ataque que solo existen por una combinación específica de sistemas constituyentes.

Los ataques complejos que utilizan datos de varios orígenes para crear un perfil de las personas se denominan doxxing. Las personas afectadas por este tipo de ataque pueden encontrar su información personal publicada en Internet, incluyendo la dirección postal, número nacional de identidad o números de teléfono, entre otros en contra de su voluntad. Los atacantes pueden recopilar esta información de una o varias fuentes, y utilizarla posteriormente para tomar decisiones sobre cómo atacar o acosar a la víctima.

En este estudio se ha analizado un tipo específico de ataque doxxing utilizando una perspectiva SdS. En este tipo de ataque la información recopilada de diferentes sistemas sobre una persona no se utiliza directamente contra las personas, sino para explotar la seguridad de las identidades de su Personalidad Digital.

Este es un problema real que cuenta con casos documentados como el que le sucedió a Mat Honan. Honan es un periodista que fue víctima de un atacante que recopiló información su personal disponible a través varios sistemas. El atacante combinó información de un sistema tras otro hasta que pudo explotar la seguridad en los sistemas donde el Sr. Honan tenía identidades. Finalmente, el atacante se hizo pasar por el Sr. Honan y borró toda su existencia digital. En trabajos anteriores [36] se han identificado problemas similares en el contexto de Sistemas de sistemas.

En este capítulo presentamos un enfoque basado en estudios relacionados [21] [28] [31] [51] para evaluar sistemáticamente la seguridad de la Personalidad Digital al considerar la Personalidad Digital como un SdS Virtual. Este enfoque ha sido diseñado para asistir en la gestión de datos y verificar la seguridad de Personalidades Digitales interpretadas como Sistemas de Sistemas, como parte del enfoque TeSSoS [37].

Con este fin, se han definido tres preguntas de investigación:

- (PI1) ¿Qué fragmentos de datos se pueden encontrar públicamente en Internet sobre los usuarios?
- (PI2) ¿Qué información se puede generar al combinar datos de diferentes fuentes?
- (PI3) ¿Podría la sobreexposición convertirse en una vulnerabilidad para la seguridad de las identidades digitales?

Para responder a estas preguntas, contextualizamos el problema y evaluamos la seguridad de SoS analizando cómo la combinación de los datos procedentes de diferentes identidades digitales puede afectar a la seguridad de pluridentidad.

Las vulnerabilidades encontradas al analizar las identidades que forman una Pluridentidad se entienden como una vulnerabilidad que surge de la combinación de los recursos compartidos entre varios sistemas que son usados para explotar la seguridad de otro. En [44] el término vulnerabilidad se ha definido como “Un defecto o debilidad en el diseño, implementación u operación y gestión de un sistema que podría ser explotado para violar la política de seguridad del sistema”. En este sentido, analizando cómo se combinan las identidades en una Pluridentidad podemos encontrar vulnerabilidades en el diseño del SdS (la Pluridentidad) empleando los propios recursos de los sistemas constituyentes (cada identidad) para infringir la directiva de seguridad del SdS.

13.1.2 Consideraciones éticas

Los datos utilizados para la validación en este estudio (Sección 13.4) se obtuvieron de una URL disponible al público que contenía información que permitía identificar y generar perfiles de personas. Después identificar este hecho, el administrador del sitio web fue notificado para ayudarles a resolver este problema. En consecuencia, eliminaron los datos de la web pública.

Nuestro objetivo no incluye utilizar estos datos para ningún propósito comercial o perjudicial, sino como un escenario real para validar el enfoque presentado, evitando el uso de datos sintéticos. Por lo tanto, realizamos el estudio sin notificar a las personas involucradas, porque su consentimiento informado o participación voluntaria habría sido una amenaza potencial para la validez. De este modo, hemos llevado a cabo este estudio sin notificar previamente a las personas involucradas, ya que su consentimiento informado, o su participación voluntaria habría supuesto una amenaza a la validez del estudio. No obstante, el estudio ha sido desarrollado con las máximas precauciones, y ni puede ni debe suponer un riesgo ni daño para los sujetos analizados. Esto se ha llevado a cabo mediante el uso seudónimos para los datos de los sujetos. En este sentido, en lugar de almacenar información real de las personas, usamos representaciones ficticias para representar a cada candidato. La actividad se ha llevado a cabo de conformidad con reg. EU 2016/679. Más concretamente, este estudio ha seguido el código de conducta y la práctica profesional específico para el tratamiento de datos personales con fines estadísticos y científicos, de conformidad con el artículo 20, apartado 4, del Decreto italiano 2018/101.

Los datos tratados durante este estudio han sido manipulados de acuerdo con los siguientes principios:

1. Publicación. El único propósito de utilizar estos datos es académico y proporcionar valor a la investigación.

2. No explotación. Los datos no se pueden utilizar para ponerse en contacto con las personas a las que se refieren estos datos de ninguna manera.

3. Caducidad. Los datos solo se pueden almacenar durante el tiempo en que se desarrolla y publica este estudio. Una vez completado el proceso de revisión y publicado el trabajo, se han eliminado todos los rastros de pluridentidad utilizados en este estudio.

4. Inocuidad. El uso de estos datos no puede comprometer la seguridad de los sujetos de ninguna manera.

5. Anonimato. Los datos analizados por las personas se anonimizarán de manera que no puedan utilizarse para identificar a quién se refieren estos datos.

6. Confidencialidad. Los datos no se pueden compartir, copiar, imprimir o distribuir. No se puede acceder a los datos por ninguna otra parte que no sean los coautores del estudio.

13.1.3 Estructura del capítulo

El resto de este capítulo se estructura de la siguiente manera: Algunos patrones relativos a la sobreexposición de la Personalidad Digital y trabajos relacionados se mencionan en la Sección 13.2. En la Sección 13.3 se describen los métodos, se introducen las definiciones y se muestran los modelos. La Sección 13.4 proporciona los resultados de validación de la aplicación del método descrito. Por último, la Sección 13.5 esboza las conclusiones.

13.2 ANTECEDENTES Y TRABAJO RELACIONADO

13.2.1 Antecedentes

Los medios a los que un atacante puede llegar a usar como fuente de datos, la información que puede deducirse de los datos y el valor de esta información influyen al determinar cuán segura es una Personalidad Digital.

Los fragmentos de datos que pueden encontrarse libremente en Internet pueden formar parte de las contraseñas o utilizarse para responder a las preguntas de seguridad planteadas en los procedimientos de recuperación de contraseñas. Entre las típicas preguntas de seguridad para recuperar el acceso cuando se ha olvidado una contraseña podemos encontrar: “¿Cuándo naciste?”, “¿Cuál es el nombre de tu mascota?” o “¿Cuál es tu destino de vacaciones favorito?”. Sin embargo, estas preguntas podrían ser fáciles de adivinar por un tercero si los sujetos tienen una actividad social activa en la red [41].

Además, pueden identificarse patrones que permitan a un tercero llegar a parte de esta información combinando datos y deducción a partir de éstos. Mirando un perfil de red social es posible leer el nombre de la persona y una imagen, que da una idea del sexo, la edad y la etnia.

Esto no supone una gran cantidad de datos, sin embargo, es suficiente para ser identificado, y permitir ataques personalizados con el objetivo de dañar o recuperar más datos, en ataques como eWhoring [22].

Por ejemplo, es posible pueda obtener la fecha de nacimiento de su víctima mediante el siguiente patrón. El día y mes de nacimiento se pueden obtener en cualquier red social leyendo los mensajes de felicitación enviados por otros usuarios. Por otro lado, el año de nacimiento se puede derivar de LinkedIn, basado en qué año comenzó un ciclo de estudios.

Además, los usuarios descuidados que publican fotos de sus mascotas en las redes sociales pueden revelar datos sensibles sobre sus preguntas de seguridad.

No sólo las cuestiones de seguridad pueden verse afectadas, sino que también la información no digital se puede utilizar para explotar el factor humano. Los atacantes podían recuperar datos a través de terceras personas mediante el uso de la información personal de la víctima en una llamada telefónica, lo que podría llevarlos a recuperar más datos.

En un caso de prueba realizado por los autores para comprobar la disponibilidad de información de personas en sistemas de terceros, hemos utilizado un stand de autoservicio que ofrece la posibilidad de imprimir recibos después de una compra. Este sistema ofrece una función de búsqueda, disponible públicamente, en la que al escribir un código fiscal permite recupera el nombre, el número de identificación fiscal y la dirección postal completa de la persona, tal como se muestra en una fotografía de la pantalla del soporte en la Figura 13.1. De esta manera, un cliente no necesita escribir todos estos datos cada vez que desea imprimir una factura. No obstante, es posible llegar a los datos de facturación de otra persona utilizando únicamente el número de IVA que puede encontrarse en una tarjeta de visita.

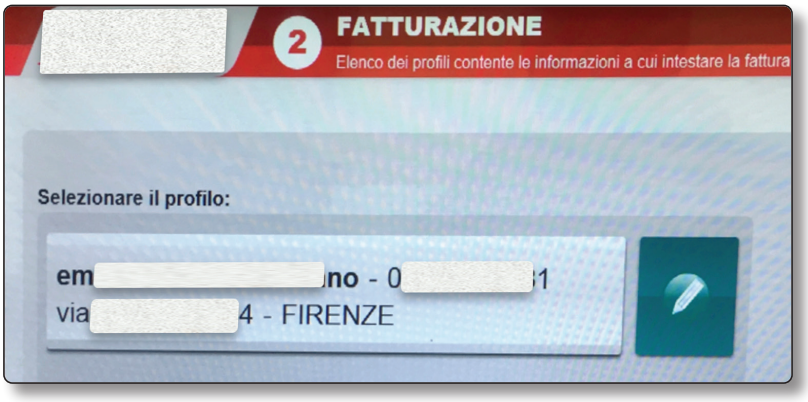

Figura 13.1. Stand de autoservicio

Combinando la información de la tarjeta de visita, y la información dada por la función de búsqueda del stand de autoservicio, pudimos llegar a un nuevo dato: la dirección postal del hogar de una posible víctima. Esto podría permitirnos usar esta información, por ejemplo, en ataques de phishing que simulan entregas de paquetes.

Un patrón bien organizado puede permitir a un atacante alcanzar datos confidenciales de las personas y usar estos datos para ejecutar ataques precisos y dirigidos. Sin embargo, el uso de estos patrones con buena intención puede convertirse en una herramienta útil para el autoanálisis que permite una detección temprana de vulnerabilidades en una PD.

Vale la pena señalar que la combinación de la información disponible de varios sistemas, sin embargo, no es nueva. Esta estrategia se basa en el uso de OSINT (Open Source INTelligence) que permite recopilar información adicional mediante el uso de conocimientos compartidos. La aplicabilidad de OSINT incluye la obtención de la geolocalización a través de una imagen. A pesar de que una imagen puede no tener la ubicación en sus metadatos, OSINT permite saber dónde se tomó una foto simplemente analizando el entorno y los datos relacionados [20].

13.2.2 Trabajo relacionado

La búsqueda de fuentes para recuperar los datos de las personas se ha analizado en varias ocasiones aplicando diversas estrategias. Hay algunos patrones recurrentes para recuperar los datos de una Personalidad Digital, siendo las redes sociales las fuentes de datos más comunes. Esto motivó a varios autores a llevar a cabo su investigación en este dominio.

Estudiando los problemas de privacidad, se realizó un estudio para determinar el uso de un mismo nombre de usuario entre los diferentes sistemas en Internet [39]. Esta línea de investigación fue continuada por Malhotra et al [28]. En su trabajo los autores se centraron en la aplicación de técnicas para medir la similitud de los perfiles de usuario en diferentes redes sociales. En el mismo año, Creese et al. [8] publicó un trabajo en el que muestran cómo la combinación de datos procedentes de diversas fuentes puede proporcionar datos adicionales y consolidar o refutar piezas de información. Se podría inferir información más fiable sobre una posible víctima al estudiar los identificadores personales de una persona, que podrían obtenerse buscando anuncios de becas escolares, o mediante su información pública si son trabajadores autónomos [21]. Los datos adicionales que los autónomos también pueden proporcionar incluyen su dirección postal al facturar, lo que reduce a un solo lugar la ubicación de la persona. Toda esta información genera conocimientos útiles sobre una persona que puede ser potencialmente utilizada para explotar la seguridad basada en el conocimiento en sus sistemas [18].

La combinación de datos fue estudiada más tarde por Minkus et al. [31]. Estos autores trabajaron en un experimento en el que combinaron lo que las personas publicaron en Facebook con los datos disponibles en otras fuentes. Como resultado, pudieron asociar información de una fuente de datos a otra para crear un perfil más preciso de esas personas.

Un estudio más reciente describe una obra en la que los autores utilizaron no sólo información disponible públicamente, sino también comportamiento de las personas [51].

Recientemente, con el aumento de los dispositivos *wearables*, en 2017 se llevó a cabo un estudio en el que los autores analizaron cómo los *wearables* también pueden constituir una rica fuente de datos personales [2].

En Europa, para proteger la privacidad de los datos del usuario, el RGPD (Reglamento General de Protección de Datos) [48] en su Art. 15 se ocupa del derecho de acceso a los datos de las personas. Las personas tienen derecho a saber cómo se procesan sus datos personales, así como el derecho a acceder a sus datos personales. Para ayudar en el uso de sus derechos, algunos servicios en línea como MDR (My Data Request) [30] ayudan a los usuarios a solicitar sus datos personales a los propietarios del sistema web. Estas leyes y servicios son útiles para que los usuarios manejen su información personal. Sin embargo, mecanismos ineficaces de autenticación permitirían a un atacante hacerse pasar por una víctima y solicitar sus datos personales a través del RGPD para obtener toda la información de esta persona. Un estudio reciente ha confirmado tal debilidad en el factor humano [11]. En este estudio las personas objetivo no son las únicas víctimas afectadas. En algunos casos, debido a un error humano, también se filtran los datos de terceras personas. Esto muestra cómo la aplicación del RGPD puede convertirse en un arma de doble cuando no se identifica correctamente al solicitante. Es posible que las personas necesiten entender cuán expuestas están sus pluridentidades ya que la sobreexposición está afectando a la forma en que las personas son identificadas al acceder a los datos protegidos por el RGPD.

Por otro lado, hay algunos servicios legítimos disponibles para las personas puedan saber si sus identidades han sido reconocidas en una fuga de datos. Estos servicios son útiles para descubrir si es necesario cambiar las credenciales de cualquier identidad en cualquier lugar de Internet. Una de estas herramientas que podría utilizarse es HIBP (haveibeenpwned.com) [19]. Otros servicios que podrían utilizarse para analizar las identidades son SpiderFoot [45] y HPI-ILC (Hasso Plattner Institute Identity Leak Checker) [23].

SpiderFoot es una herramienta de reconocimiento semiautomática que ejecuta consultas en diferentes orígenes de datos abiertos y recupera coincidencias

para las consultas de entrada. Esta herramienta busca la conexión de las identidades a través de las fuentes consultadas e intenta descubrir cualquier coincidencia o conexión entre ellas, revelando también dónde se utiliza una identidad.

HPI-ILC es una herramienta más sencilla que permite consultar por dirección de correo electrónico. Proporciona datos personales relacionados como número de teléfono, fecha de nacimiento o dirección postal que se ha hecho público en Internet a través de filtraciones de datos. La ventaja de este servicio, a diferencia de HIBP, es que HPI-ILC permite saber qué otros datos podrían hacerse públicos en la fuga. Además, este servicio protege el anonimato de la persona, enviando el informe directamente a la dirección de correo electrónico consultada, evitando la divulgación de datos a personas curiosas.

En el peor de los casos, incluso es probable encontrar algunos casos de registros almacenados en sistemas de terceros como Pastebin.com, en el que los hackers publican las fugas de datos que obtienen. Desafortunadamente, los atacantes pueden aprovechar el uso de estos datos contra sus víctimas.

13.2.3 Comparación con el trabajo relacionado

Se han descrito varias técnicas para ejecutar la recopilación de datos, pero éstas sin embargo no ofrecen una estructura explícita para controlar los datos. Hasta donde sabemos, a pesar de que existen herramientas y estrategias para recuperar y analizar los datos públicos disponibles, no existen mecanismos para analizar o comprender el impacto de la sobreexposición en la Pluridentidad entendiéndola como un Sistema de Sistemas.

El concepto de Pluridentidad que aplicamos para definir un grupo de identidades que representan a una sola persona es como el propuesto en [21]. Introdujeron el concepto de *super identidades* como un conjunto de elementos individuales de algunas identidades. Por el contrario, este estudio se ha basado en el uso de una perspectiva novedosa, que considera cada fuente de datos participante como un sistema constituyente en un Sistema de Sistemas. La principal diferencia es que en nuestro enfoque no estamos creando una nueva super *identidad, sino* que estamos armando todas las identidades como sistemas constituyentes bajo el prisma SdS. Las vulnerabilidades que surgen al combinar los recursos de los sistemas constituyentes son, por lo tanto, comportamientos *emergentes* de un SdS que descienden de un defecto en su diseño.

Trabajos anteriores ponen de relieve el riesgo de tener datos públicos y cómo los datos podrían ser utilizados contra las personas. Estos estudios, sin embargo, no proporcionan un ejemplo claro sobre cuán vulnerables son las personas. El estudio

de validación realizado en este capítulo, mediante el uso del método descrito, ha detectado vulnerabilidades de seguridad debido a una sobreexposición que solo existe al combinar ciertas identidades.

En resumen, en este estudio ampliamos investigaciones previas sobre la recopilación de datos para proponer el método *de análisis de representación de personajes de pluridentidad digital* que estandariza la recopilación de datos y el análisis de seguridad, y el modelo de conocimiento de la persona *digital* y el modelo de seguridad *relacional,* que estructuran y analizan los datos recopilados.

Un procedimiento regulado que favorece la creación de una métrica para evaluar la exposición de una persona. Este enfoque puede sistematizarse y automatizarse parcialmente, lo que puede ayudar a las personas a autodeterminar su configuración de Pluridentidad para detectar posibles violaciones de su seguridad.

13.3 ARP2D

Se ha diseñado un método denominado Análisis del Retrato de la Pluridentidad de la Personalidad Digital (ARP2D; en inglés: *Digital Pluridentity Persona Portrayal Analysis, DP3A*) para analizar si la información disponible sobre las identidades podría amenazar la seguridad de la Personalidad Digital. Este método se ha estructurado en dos fases cíclicas. La primera fase se basa en la recopilación de datos: es decir, la recopilación de información de diferentes fuentes y la elaboración de un perfil de la Personalidad Digital. A continuación, los datos se combinan y se utilizan para crear información sobre las identidades que mejora el conocimiento sobre la Personalidad Digital (PD). La segunda fase desafía la seguridad de los sistemas utilizados por la PD mediante el uso de la información y el conocimiento que ha generado.

13.3.1 Definiciones

Algunos términos clave deben definirse antes de describir el método ARP2D. Algunas de las definiciones expuestas en este estudio son una extensión de las definiciones ya dadas en obras anteriores [12] [7] [46].

1. Una *identidad* es la representación virtual de una entidad (por ejemplo, su cuenta de correo electrónico). Una identidad está asociada a una entidad a través de un identificador.

2. Un *identificador* es un elemento de datos cuyo propósito es distinguir de forma única una entidad dentro de un contexto (por ejemplo, una dirección de correo electrónico).

3. Un *fragmento de datos* es una porción de datos que pertenece a una entidad o identidad (por ejemplo, un apellido).

4. Un *proveedor de identidades* es un sistema que es capaz de generar identidades que se pueden utilizar en varios sistemas (por ejemplo, Gmail).

5. La *pluridentidad* es una condición que hace referencia a una entidad, que está representada por más de una identidad (por ejemplo, una cuenta de correo electrónico y su cuenta de Instagram).

6. Un *usuario* es una entidad que desea acceder a algunos recursos del sistema, generalmente mediante una identidad (por ejemplo, usted).

7. Un *registro* o *registro de datos* es un conjunto de elementos de datos almacenados en uno o varios sistemas que hacen referencia a una entidad, identidad o pluridentidad en particular (por ejemplo, sus fotos en Instagram).

8. Una *Personalidad Digital* es un registro lo suficientemente rico en fragmentos de datos como para proporcionar una representación adecuada de la entidad o identidad representada (por ejemplo, nuestra actividad en redes sociales o los correos electrónicos se envían).

9. Una *representación* es el resultado de representar una Personalidad Digital, al tener un rastro de cada elemento de datos que conforma el registro (por ejemplo, un documento que resume los registros pertenecientes a su Personalidad Digital).

Teniendo en cuenta estas definiciones, la primera fase del ARP2D se denomina Retrato de la Personalidad Digital (RPD, en inglés: *Digital Persona Portrayal, DPP), que* tiene como objetivo describir los datos recopilados de diferentes identidades y darles un significado. A continuación, el *Análisis de Seguridad de Personajes Digitales (*ASPD, en inglés: *Digital Persona Security Analysis)* busca utilizar datos recopilados anteriormente para explotar la seguridad de los sistemas empleados por la Personalidad Digital. En las secciones siguientes, se describen estas dos fases.

13.3.2 Representación digital de personajes de pluridentidad

El Retrado de la Personalidad Digital (RPD) está inspirado en la fase de recopilación de información definida por Mouton et al. [33], basada en el ciclo de ataque de ingeniería social descrito por Mitnick y Simon [32]. Mouton et al. definieron en su trabajo un marco de ataque de ingeniería social. Se describieron seis fases que componen aquellas actividades identificadas que definen el comportamiento de un atacante. Después de realizar la "identificación de objetivos", los autores describen la fase de recopilación de información con tres actividades iterativas: (i) identificar las fuentes, (ii) recopilar información de las fuentes, (iii) evaluar la información recopilada.

Durante el RPD, se identifican las fuentes, se recopila y evalúa la información, en esencia se retrata una PD. Retratar una PD consiste en analizar cada identidad que compone la pluridentidad de la Personalidad Digital. En este análisis de la Personalidad Digital, se recopilan elementos de datos y se describen los requisitos de seguridad para cada sistema en el que se utilizan las identidades.

Se ha diseñado un modelo para organizar y combinar los datos recopilados procedentes de cada sistema constituyente. El modelo ha sido nombrado metamodelo de representación de personalidades digitales y es una extensión del Metamodelo de Clase de UML [38].

En la siguiente sección se describen las actividades que retratan a un DP mediante el Metamodelo de Representación de Personalidades Digitales, que se utilizará más adelante durante el Análisis de Seguridad de Personajes Digitales.

13.3.2.1 METAMODELO DE REPRESENTACIÓN DE PERSONAJES DIGITALES

El Metamodelo de Representación de Personajes Digitales (MRPD) se muestra en Figura 13.2. Se utiliza para estructurar los registros de datos (RD) de una PD. Este modelo incluye siete clases:

1. La **Personalidad Digital** (PD), en la esquina superior izquierda, se compone de un conjunto de Identidades y Registros. Una PD es una clase que representa la entidad cuya seguridad se está analizando. El PD se identifica por un nombre y puede tener dos elementos asociados: las identidades y los registros.

2. Las **identidades**, en la esquina superior derecha, están asociadas a uno o más sistemas. Las identidades se pueden distinguir por la dirección de correo electrónico, el número de teléfono, los datos biométricos, etcétera, siendo el correo electrónico el identificador más común [16] [34] [50].

3. Los **sistemas**, en el centro a la derecha, que comparten la misma identidad están funcionando en el mismo contexto. Se puede acceder a un sistema a través de diferentes identidades pertenecientes a la misma PD. Los sistemas pueden contener registros sobre la PD. Algunos registros pueden incluir datos personales que podrían llevar al atacante a obtener información sobre la identidad física de la víctima. El sistema también puede ofrecer algún mecanismo de seguridad que, en caso de una autenticación correcta, ofrece acceso privilegiado a algunos datos o acciones. Sin embargo, la autenticación de identidad no es obligatoria en todos los sistemas. Esto se debe a que existen sistemas que proporcionan datos sensibles sin necesidad de autenticación de identidad, como WHOIS, becas escolares o sitio web de trabajo, entre otros. Según los autores de [25], estos sistemas son un objetivo de ataque potencial para más de un PD.

4. A la mitad izquierda, los **registros** de datos procedentes de diferentes sistemas se pueden combinar aplicando algunos conocimientos sobre la PD que generan a su vez nuevos fragmentos de datos que podrían mejorar los conocimientos previos. Los registros se pueden utilizar total o parcialmente para explotar sistemas cuya seguridad está basada en el conocimiento. Las PP.DD. pueden proporcionar registros sobre terceras PP.DD., que pueden exponer indirectamente sus identidades.

5. La **autenticación de identidad**, en la parte media inferior, es un mecanismo de seguridad responsable de comprobar si la identidad coincide con la entidad que tiene acceso a estos privilegios. La autenticación podría realizarse utilizando conocimientos (es decir, lo que la persona conoce) o artefactos (es decir, lo que la persona posee). La autenticación también se puede extender a la biometría (es decir, lo que la persona es), pero en este estudio consideramos sólo conocimiento y artefactos.

6. **Conocimiento**, en la parte inferior esquina izquierda, es un subtipo de autenticación de identidad. Su fortaleza reside en el uso de un secreto que terceros no puedan saber. La autenticación basada en el conocimiento típicamente se basa en el uso de contraseñas. Este conocimiento no debe encontrarse en los registros de cualquier otro sistema de la Pluridentidad de la PD. Sin embargo, en algunos casos hay sistemas que pueden proporcionar datos suficientes para generar este conocimiento, que crearía vulnerabilidades importantes.

7. **Artefacto**, en la esquina inferior derecha, es un subtipo de autenticación de identidad. La fuerza reside en el uso de un sistema, que puede ser

digital o analógico. Recibir un correo electrónico en la bandeja de entrada o un SMS en un teléfono móvil son ejemplos de autenticación de identidad basada en artefactos. Estos sistemas delegan la responsabilidad de la seguridad en la seguridad de otro sistema que incluso puede pertenecer a otra PD. Tener derecho de acceso al sistema delegado otorga automáticamente acceso a todos los demás sistemas de los que el primero sea responsable.

13.3.2.2 RETRATO DE LA PERSONALIDAD DE PLURIDENTIDAD DIGITAL

El retrato de la Personalidad Digital parte de información conocida sobre la PD. Estos datos iniciales se toman como punto de partida para buscar en cualquier sistema en el que se pueda explotar una identidad del PD: por lo tanto, se ejecutan búsquedas en Internet para encontrar evidencias de identidades relacionadas con la PD.

Cuando se detecta una identidad, el sistema que la incluye se evalúa dos veces. La primera evaluación consiste en considerar los registros proporcionados por los sistemas en el contexto del llamado Modelo de Conocimiento de la *Persona Digital (*MCPD*, en inglés: Digital Persona Knowledge Model DPKM)*. Por otro lado, las características de seguridad del sistema se consideran y modelan como un *Modelo de Seguridad Relacional (*MSR*, en inglés: Relational Security Model)* que se centra en la seguridad entre los sistemas y sus dependencias.

MCPD y MSR son submodelos pertenecientes al modelo MRPD que se muestran en Figura 13.2. Cada submodelo tiene un propósito específico y su separación se ilustra en la Figura 13.2 La parte superior, que contiene Personalidad Digital, Identidad, Registro de Datos y Sistema, corresponde al submodelo MCPD, que se utiliza para organizar los registros asociados a una PD según la identidad y el sistema.

La parte inferior, que contiene registro de datos, sistema, autenticación de identidad, conocimiento y artefacto, corresponde al submodelo MSR, cuyo propósito es definir los mecanismos de seguridad que protegen a la pluridentidad, es decir, protegen el SdS.

Ambos submodelos permiten un análisis de todos los registros de todos los sistemas por completo, que se pueden utilizar para identificar una combinación de datos de diferentes sistemas que explota la seguridad del SdS.

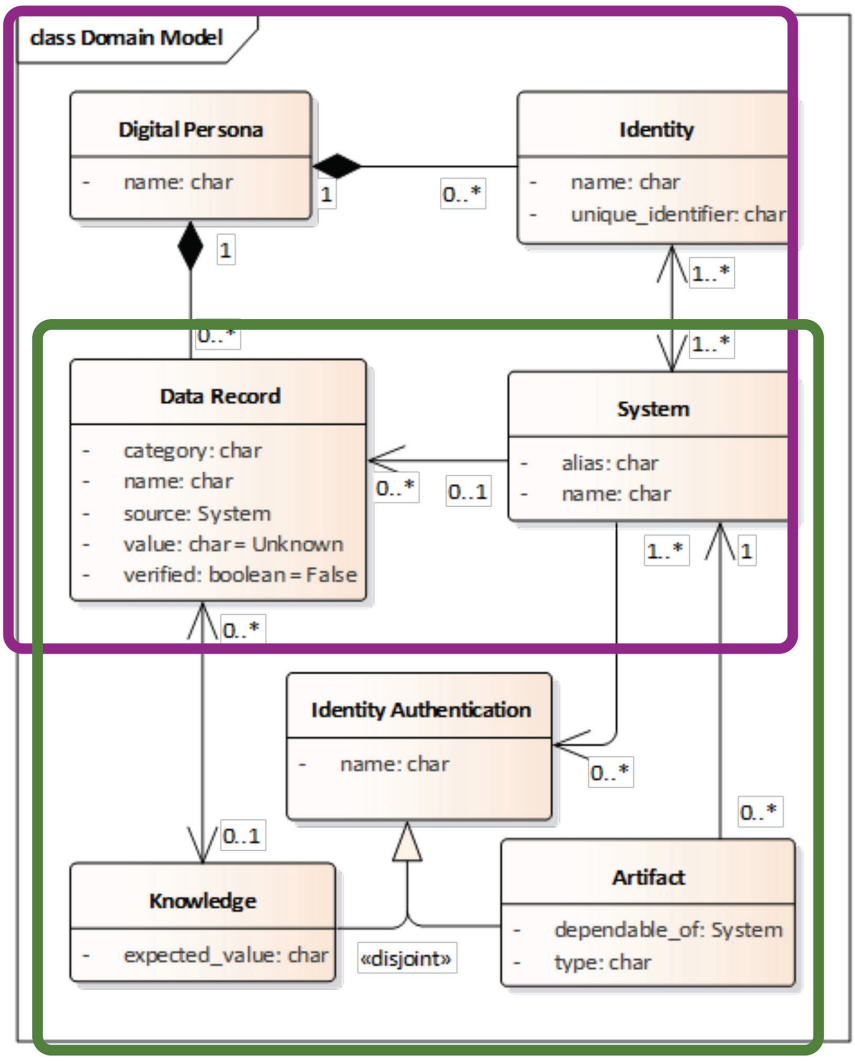

Figura 13.2. MCPD y MSR

Además, la autenticación de la identidad se puede utilizar como criterio para restringir la búsqueda de registros. Dado que la motivación para modelar la PD es explotar la seguridad en el SdS, los elementos de datos que no son relevantes para explotar la seguridad en los sistemas pueden no ser considerados. Figura 13.3 ilustra cómo se entiende un sistema como una combinación de características de la PD y su seguridad, y cómo cada parte corresponde a MCPD o MSR, respectivamente.

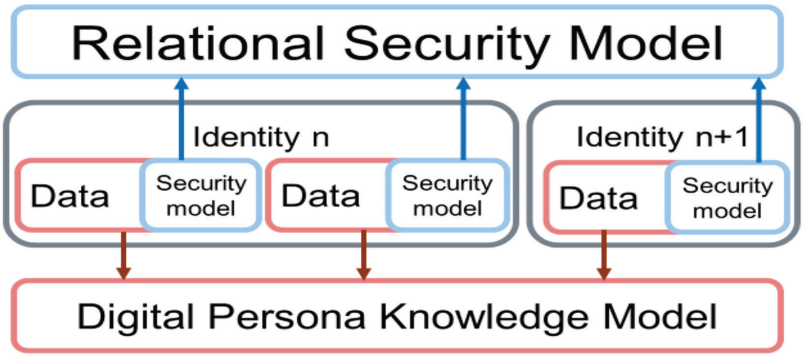

Figura 13.3. Dicotomía de datos y modelos de seguridad

Durante el proceso de retrato, el MSR se actualiza cada vez que un nuevo sistema del PD se encuentra. Esta actualización es necesaria para refinar la información suficiente para autenticarse en los sistemas basados en el conocimiento. De este modo, el MCPD se puede consultar de nuevo para recuperar cualquier registro de datos que pueda ser relacionados con la seguridad usada en el sistema recién encontrado. Los sistemas se consultan por orden de aparición, buscando registros de datos y autenticación de identidad. Cada vez que un registro de datos revela una nueva identidad en un nuevo sistema asociado a la PD tiene (p. ej., una publicación de Facebook revela que una foto está disponible en una cuenta de Instagram), éste nuevo sistema se añade a la cola y el proceso continúa. El proceso termina cuando no hay sistemas pendientes de ser analizados. La Figura 13.4 describe esta estrategia.

Al buscar identidades de una PD se pueden considerar dos métodos alternativos. (1) Un método en el que el analista evita el uso de datos conocidos de antemano y limita la búsqueda en los datos iniciales y encontrados. Este método de búsqueda a ciegas imitaría a un atacante, es decir, sin ninguna información detallada sobre la víctima. (2) En otro método, se lleva a cabo una búsqueda completa utilizando todos los conocimientos sobre la PD. Al usar conocimientos previos, se puede generar un modelo más completo. Este caso simularía un autoanálisis.

Las vulnerabilidades encontradas al analizar los MCPD y MSR se entienden como vulnerabilidades que surgen mediante la combinación de los datos de ciertos sistemas que permiten explotar la seguridad de otro. Por lo tanto, mediante el uso de estos dos modelos podemos encontrar vulnerabilidades en el diseño de un SdS que se originan de los recursos compartidos entre los sistemas constituyentes y que podrían violar la seguridad del SdS.

Modelo de Conocimiento de la Personalidad Digital

Al buscar datos sobre una PD, el submodelo MCPD se utiliza para el análisis de información que proporciona conocimiento sobre la PD.

MCPD se centra en los registros del MRPD y se utiliza para categorizar los elementos de datos que podrían utilizarse para explotar la seguridad de los sistemas.

Para un mejor manejo de los datos encontrados, se proponen algunas categorías predefinidas que organizan los registros de acuerdo con su naturaleza, como, por ejemplo: identificadores, demografía, ubicación, profesión, educación, económica, social, salud o intereses entre otros.

Esas categorías se basan en los utilizados para organizar los datos en los censos de algunos países[5,6,7]. No obstante, estas categorías pueden adaptarse para un mejor ajuste al contexto analizados. La Figura 13.5 muestra un MCPD anonimizado como resultado de un caso de estudio. En esta figura, los registros de datos se organizan columnas, representando categorías y cada sistema como una fila. De esta manera cada registro público se organiza en una matriz que se puede estudiar para detectar vulnerabilidades si estos registros fueran utilizados como autenticación de identidad en el MSR.

Modelo de seguridad relacional

El modelo de seguridad relacional (MSR, *en inglés RSM*) se centra en los sistemas y su seguridad. El objetivo de este submodelo es organizar los sistemas que utilizan la misma identidad y señalar qué sistema es el proveedor de identidades. En el MSR, para cada sistema la seguridad se describe según sus características conocimiento o artefacto. Este modelo se utiliza para guiar el modelado MCPD, ya que el objetivo de MCPD es identificar suficientes datos que permitan generar información y conocimiento que podría emplearse para explotar la seguridad detallada en el MSR. La Figura 13.7 muestra una versión anonimizada de un MSR generado para un caso de estudio. En este modelo se identifica cada sistema, así como su sistema responsable, es decir, el proveedor de identidades. En este modelo, para cada sistema encontrado, se enumeran los mecanismos de seguridad utilizados. Los sistemas se organizan de acuerdo con la identidad que se utiliza en los sistemas.

---

5 https://www.census.gov/acs/www/data/data-tables-and-tools/data-profiles/2017/

6 https://www.ine.es/welcome.shtml

7 https://ec.europa.eu/eurostat/web/ess/

Alice Smith

Demographics and identifiers		Location	Profession	Education	Economical	Social	Health	Interests
Twitter	@smith_alice	Springfield						Joined dec 2009
	Alice Smith							
	facebook: nickname0							
Instagram	alicesmith_0	Springfield						Basket
	facebook: alicesmith0					Springfield Basket Club		
Google+	Telephone: PHONE_NUMBER							
	Birthdate: December 20th							
LinkedIn	Alice Smith	Lives in Sprinfield	Work in Nuclear Plant	Studied in University of Springfield				
				Started university in 2002				
				Probably born in 1984				
Facebook	nickname0	Works in Springfield	Works in Nuclear Plant	Studied in Shelbyville		Owns a dog		Likes number 0
	alicesmith0	University located in Springfield	Worked in Teaching	Studied in Springfield		Goes to beach with girlfriend		Likes basket
		Summer beach in Shelbyville	Worked as Researcher			Goes to beach with friends		Likes beaches
						Goes to beach with dog		Owns a car (Brand and model)
iCloud	alice_smith@hotmail.com							Potentially user of iPhone
Hotmail	alice_smith@hotmail.com							
	Telephone: PHONE_NUMBER							
	al***@gmail.com							
Leaks	alice_smith@hotmail.com							
	alice_smith@hotmail.com:Nic*****							
	alice_smith@hotmail.com:nic*****							
	alice_smith@hotmail.com:ABC*****							

Figura 13.4. MCPD de Alice

Figura 13.5. Estrategia del PDPM

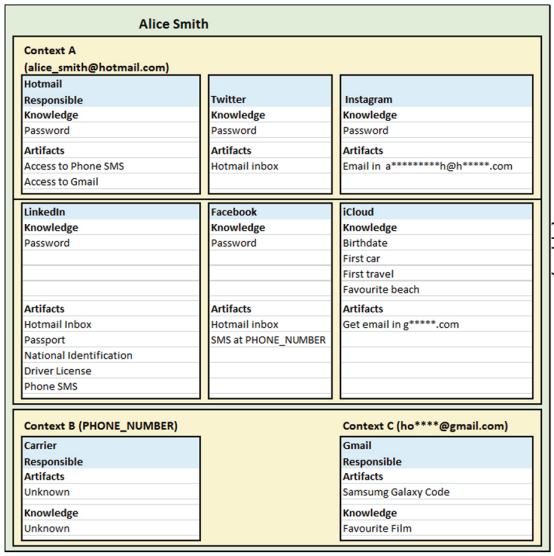

Figura 13.6. MCPD de Alice

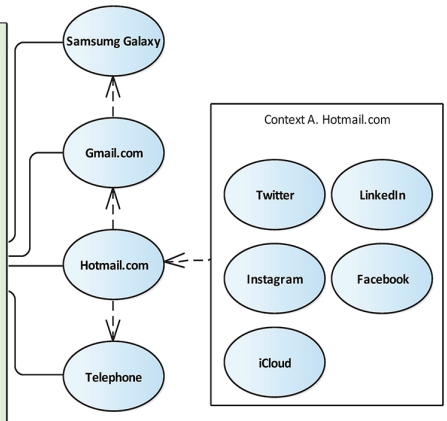

Figura 13.7. Estrategia del PDPM

Un sistema puede aparecer más de una vez representado en el modelo si una Persona Digital con Pluridentidad usase el mismo sistema con identidades diferentes.

En cuanto a la seguridad basada en artefactos, mediante el estudio de las dependencias entre los sistemas especificados en el MSR, se puede describir una jerarquía de dependencias. Esta cadena de sistemas nos permite comprender qué sistemas tienen una mayor responsabilidad y, por lo tanto, aquellos que deben producir mecanismos de seguridad más sólidos.

Las dependencias entre sistemas que se han identificado en el MSR de la Figura 13.7 se han descrito como un modelo de caso de uso en la Figura 13.6. Para esto se ha representado como caso de uso aquellos sistemas cuya seguridad depende de otros sistemas.

13.3.3 Análisis digital de seguridad de la persona

Una vez completado el MRPD, a través de una combinación de un MCPD y un MSR, podrían inferirse otros datos que revelarían nuevos vectores de ataque.

Los vectores de ataque potenciales se pueden identificar mediante el análisis de otros sistemas ya existentes que funcionarían como fuente de registros. Por ejemplo, como se ha mencionado previamente, un conjunto de mensajes de felicitación en un

día en particular podría revelar el día y el mes de nacimiento. Por otro lado, el año de nacimiento podría extraerse al analizar otros factores, como, por ejemplo, cuando se comenzó la escuela secundaria o la universidad. De esta manera, cualquier pregunta de seguridad con respecto a la fecha de nacimiento puede responderse, y por lo tanto los sistemas que utilizan esta información pueden considerarse inseguros [41] [18].

Gross et al. identificaron en su trabajo [17] cómo algunas personas no se preocupan por los riesgos que implica hacer públicos sus datos, y prefieren recibir una amplia retroalimentación social.

Las personas pueden usar secretos para su seguridad basada en el conocimiento. No obstante, los atacantes podrían lanzar ataques de ingeniería con el objetivo de recuperar estos datos en particular. Cuanta más información esté a disposición del atacante y pueda usar, más sofisticado podría ser el ataque y, por lo tanto, más difícil será detectar los ataques.

Las estrategias defensivas para proteger los sistemas pueden incluir la eliminación de información que comprometa a los sistemas, identidades o registros sensatos a un atacante. Sin embargo, ocultar datos repentinamente puede despertar sospechas de que hay algo valioso digno de ocultar. Esto provoca el efecto colateral de hacer que la gente tenga curiosidad acerca de qué datos estaban allí antes, aumentando la motivación para acceder a ellos. Un atacante recopilando datos al hacer doxxing puede pasar por alto algunos detalles, sin embargo, tratar de ocultarlos puede hacer que cobren relevancia, atrayendo más atención y produciendo el efecto contrario. Esto se conoce como el efecto Streisand [8].

El análisis de un MRPD podría generar métricas de exposición del DP de acuerdo con la cantidad de información que se podría encontrar. Esta métrica podría evaluar y comparar la seguridad de las identidades de un DP y establecer si un DP es más vulnerable que otros para recibir ataques.

13.4 EVALUACIÓN

El ARP2D método ha sido evaluado en 17 sujetos anónimos para validar la efectividad y eficacia del enfoque al detectar vulnerabilidades en la seguridad de las pluridentidades. Este estudio comenzó solamente con direcciones de correos electrónico como dato conocido sobre cada DP. El objetivo de este estudio es recopilar tantos datos como fuera posible de los sujetos y evaluar si su seguridad

8 https://en.wikipedia.org/wiki/Streisand_effect

está o puede verse comprometida (con referencia a los dos métodos descritos en la Sección 14.3.2.2, utilizamos la búsqueda ciega). Por razones éticas, no se han llevado a cabo ataques reales o doxxing, y no se ha interactuado con los candidatos, ni con sus sistemas o identidades más allá de documentar sus requisitos de seguridad o recuperar datos públicos.

La evaluación se ha estructurado en tres etapas:

1. **Configuración**. Se decide el proceso seguido para seleccionar las PDs candidatas;

1. **Ejecución.** Los datos recopilados para cada PD se organizan de acuerdo con el MRPD;

1. **Análisis de datos.** La última etapa es analizar el MRPD producido para cada candidato para detectar cualquier problema de seguridad.

A continuación, incluimos una subsección separada para cada etapa y concluimos la sección discutiendo las amenazas a la validez.

13.4.1 Configuración del SoS

La validación del modelo MRPD y del proceso ARP2D se ha llevado a cabo en una población de 5234 usuarios disponibles a partir de una filtración de datos de un servicio internacional de encuestas en línea.

La herramienta SpiderFoot HX [45] se utilizó durante su fase beta privada para facilitar el análisis de los candidatos, ya que es un número prohibitivo para un análisis manual. Esta herramienta recopiló datos consultando un conjunto de API públicas usando las direcciones de correo electrónico que se le proveyeron. El propósito de utilizar esta herramienta es automatizar el primer escaneo de las direcciones de correo electrónico. Precisamente, SpiderFoot HX permitió dos lotes de consultas de hasta 300 entradas diferentes, que se dividieron en 18 sets. 600 direcciones de correo electrónico estaban siendo examinadas simultáneamente. Con duraciones que oscilaron entre 2 horas y 41 minutos a 6 horas y 40 minutos, se necesitó un tiempo total de 19 horas y 13 minutos, repartidos durante tres días, para completar este proceso de escaneo automático. Los datos relativos a cada lote de direcciones de correo electrónico se recuperaron en un archivo de tipo *.csv comprimido de aproximadamente 2Mb. El mismo expediente sin comprimir alcanzó los 200 Mb de media para los 300 candidatos.

En general, según los resultados de SpiderFoot HX, todo el conjunto de candidatos estaba utilizando 510 sistemas diferentes, con un total de 33174 conexiones entre usuarios y sistemas. El 69,76% de los candidatos utilizan desde 2 hasta 6 sistemas con la misma identidad. Entre ellos, pudieron producirse falsos positivos debido a identidades homónimas, es decir, el mismo nombre de usuario puede pertenecer a diferentes entidades; o debido a un comportamiento inusual en los perfiles sociales [35]. Estos casos fueron tratados en la siguiente etapa mediante un análisis manual.

Tras un primer análisis de la fuga de datos usada como fuente de datos, se detectaron 4237 direcciones de correo electrónico válidas. Las 941 entradas restantes eran números de teléfono, nombres o direcciones de correo electrónico inválidas. No obstante, ya que 4237 es un número elevado de personas para aplicar manualmente la propuesta, se estableció un criterio para seleccionar un grupo reducido de casos.

Se desarrolló un script en Python para leer automáticamente el archivo CSV generado por Spiderfoot y extraer información relevante. Este script se puede encontrar en un repositorio público de GitHub[9], en cambio debido a la naturaleza de los datos de los archivos csv, esos archivos no se pueden publicar ni referir en este estudio. El script reveló que muchos registros de datos habían sido revelados en filtraciones de datos bien conocidas (por ejemplo, "*collection4g*", "*collection4eu*", "*collection4u*", "*onlinerspambot*", "*collection1*", "*exploit*"). Se decidió omitir estos sistemas de nuestro análisis, a pesar de que estos datos pueden generar una enorme vulnerabilidad para el DP, ya que estos sistemas no son gestionados por los usuarios. Estas filtraciones involucraron a 1664 (38,76%) identidades, que aparecieron en al menos una fuga. El 61,23% de las filtraciones involucraban identidades gestionadas por Hotmail (1019 identidades), el segundo proveedor de identidad más afectado fue Gmail con el 29,63% de las filtraciones (493 identidades). Se encontraron un total de 134 diferentes proveedores de identidad digital entre los analizados. A pesar de la diversidad, más del 93% de la población utiliza los mismos 5 principales proveedores de identidad. Estos cinco principales proveedores de identidad utilizados por los usuarios del sistema de encuestas en línea se muestran en la Tabla 13.1.

En general, cuanto mayor sea el número de redes sociales en las que aparecen las personas, más expuestas están. De hecho, las redes sociales son una fuente útil para extraer datos sobre alguien y sus amigos o seguidores [18] [51]. Por lo tanto, en este estudio decidimos seleccionar aquellos usuarios que fueron identificados por el motor SpiderFoot en Facebook, Instagram, Twitter y LinkedIn. A partir de un análisis de los resultados de SpiderFoot, 17 personas se seleccionaron por estar utilizando esas redes sociales.

---

9 https://github.com/miguel-olivero/Spiderfoot-Analyzer

El proceso ARP2D se aplicó a estos 17 sujetos, tomados como representantes del usuario activo promedio en internet. El estudio continúa con un estudio manual de estos candidatos potencialmente más expuestos.

Después de recopilar los datos del DP, el estudio continúa con el uso del MCPD para analizar los registros de datos DP y el MSR para analizar la seguridad en los sistemas.

Principal proveedor de identidades	Usuarios
hotmail.com	2372 (55,98%)
gmail.com	1271 (29,99%)
yahoo.es	133 (3,13%)
hotmail.es	120 (2,83%)
msn.com	51 (1,20%)

Tabla 13.1. Los 5 principales proveedores alternativos de identidad

13.4.2 Ejecución de ARP2D

Para cada candidato seleccionado, comenzamos el retrato de la pluridentidad de la PD empleando los modelos. Creamos una instancia de un modelo MRPD para cada sujeto, lo que nos permite analizar los datos encontrados y los mecanismos de seguridad que se utilizan en cada sistema. El proceso se inició analizando los mecanismos de seguridad del proveedor de identidades y buscando sistemas en los que se pudiera utilizar el conocimiento necesario. Como se mencionó previamente, se aplicó una estrategia de búsqueda a ciegas y no se estableció ningún contacto con las personas. Esta decisión fue motivada para evitar que, al detectar de que sus datos están siendo analizados, podrían hacer algunas modificaciones que pudieran invalidar nuestro estudio. Las personas son cada vez más conscientes de la privacidad, los riesgos que conlleva la información disponible públicamente, y su reacción podría afectar a los resultados [26] [5].

Durante el proceso, aparecieron nuevas identidades relacionadas con el DP que se estaba estudiando. Cada vez que se descubre un nuevo sistema o identidad, los datos de los sistemas ya analizados se examinan de nuevo, tratando de obtener datos suficientes que permitan explotar la seguridad de la pluridentidad. Los sujetos fueron analizamos de uno en uno hasta que no se pudieron recuperar más datos de ellos.

Señalamos que esta fase de ejecución se ha llevado a cabo únicamente mediante el uso de datos públicos, sin utilizar fugas de datos (más allá de la fuente original de los datos utilizados) o explotando cualquier sistema para adquirir más información sobre los candidatos, como se declaró en las consideraciones éticas. Esta limitación se mantuvo permanentemente a pesar de que en algunos casos habría sido posible recuperar fragmentos de datos que podrían exponer dramáticamente la seguridad de la PD y sus identidades. Es conveniente resaltar que un atacante malicioso no habría tenido tal consideración, y por lo tanto los riesgos reales podrían ser más altos que los evaluados.

Este caso de estudio se ha utilizado para responder a las preguntas de investigación que dirigen esta investigación (Sección 13.1.1).

Relativo a la PI1 "¿Qué fragmentos de datos se pueden encontrar públicamente en Internet sobre los usuarios?"

Se analizaron los datos recogidos en el MRPD y se pudo determinar: la ubicación física de 10 candidatos (58%), la posición de trabajo de 8 (47%), los intereses de 6 de ellos (35%), y la educación o formación, así como algunos detalles económicos, de 3 candidatos (17%). También se recuperaron imágenes de algunas caras. Las caras encontradas también se utilizaron como fuente de información para llevar a cabo una búsqueda inversa empleando las imágenes y proporcionar información adicional sobre las personas [40]. Un total de 8 caras fueron encontradas y utilizadas, lo que permitió la identificación facial del 47% de los candidatos.

Al final del análisis de los 17 candidatos, se revelaron un total de 40 identidades diferentes, con un promedio de cada candidato de 2,35 identidades. En total se identificaron 82 sistemas que permitieron recuperar datos personales de los propietarios del correo electrónico.

Teniendo estos datos de los candidatos, los datos se combinaron para generar más datos.

Los resultados de la aplicación del ARP2D sobre los 17 candidatos se resumen en la Tabla 13.2. En esta tabla, para cada candidato y cada categoría, se coloca una "Y" si se encuentran los datos pertinentes y podrían ser explotados, una "N" si no se encuentran datos relevantes y una "P" si los datos revelan parcialmente cualquier información pertinente.

De acuerdo a esta tabla, el sujeto #6 es el candidato más expuesto, ofreciendo datos suficientes para una identificación completa tras examinar su PD, es decir, su Sistema de Sistemas.

Las causas detectadas que ayudaron a recopilar información de estos sistemas han sido:

- Los candidatos publicaron su dirección de correo electrónico para ser contactados y recibir comentarios.
- El nombre del candidato aparece en la dirección de correo electrónico.
- Los candidatos utilizan el mismo nombre en la dirección de correo electrónico y en las redes sociales.
- Los candidatos utilizan identidades alternativas como métodos de recuperación, que se revelan cuando se utiliza "Olvidé mi contraseña".
- La dirección de correo electrónico aparece en una filtración que revela los intereses de los candidatos.
- Su dirección de correo electrónico se publica en sitios web personales o sitios web de trabajo, como GitHub.
- Los candidatos compartieron información que permitieron navegar de una red social hasta otra.
- Los candidatos utilizan la misma imagen de perfil en varios sistemas.
- Los candidatos están utilizando un mismo nombre de usuario en diferentes sistemas.
- Los candidatos tienen un puesto relevante en una empresa que aparece en documentos públicos del gobierno.

En cambio, los sujetos #2, #7, #10 y #17, fueron los más ocultos. No fue posible obtener información adicional sobre sus identidades.

El uso de una identidad que no proporciona suficiente información reduce las posibilidades de que un atacante llegue a más datos. Esto también ayuda a evitar ser rastreado a otros sistemas u otras identidades, lo que podría mejorar la seguridad de esos PDs.

Por otro lado, las identidades homónimas dificultan el seguimiento. El uso de la búsqueda automatizada para determinar el uso de sistemas por dirección de correo electrónico no fue un resultado concluyente, ya que diferentes entidades de diferentes sistemas estaban utilizando el mismo identificador.

Las razones para tener dificultades para recopilar información sobre los candidatos han sido:

- Pocos datos disponibles para iniciar la representación desde la dirección de correo electrónico.
- No se encontró ninguna red social.
- Redes sociales privadas.
- Ya no existe el dominio de la dirección de correo electrónico.
- No hay datos de contacto disponibles para blogs o dominios privados.

Durante el análisis de cada sujeto, se ha creado un modelo MRPD como una combinación de un MCPD y un MSR. El uso de MCPD y MSR nos ayuda a responder la PI2:*"¿Qué información se puede generar al combinar datos de diferentes fuentes?"*

Precisamente, el modelo MCPD ayudó a recopilar toda la información disponible y el modelo MSR guio el proceso de recopilación, limitando el alcance y centrándose en los datos pertinentes. Figura 13.5 y la Figura 13.7 muestran los modelos MCPD y MSR de un candidato anónimo al que nos referimos como Alice. Al hacer coincidir los datos recopilados del MCPD y las autenticaciones de identidad del MSR, nuestro objetivo es detectar posibles vulnerabilidades de seguridad.

Teniendo en cuenta su pluridentidad, Alice estaba proporcionando datos como nombre, dirección de correo electrónico, año de nacimiento, número de teléfono, ciudad, donde estudió, lo que estudió, mascotas y deportes. Estos datos se pueden utilizar para enviar ataques específicos para recuperar más datos y así hacer que Alice y su SoS estén cada vez más expuestos.

Se encontraron tres identidades para el DP de Alice, y ocho sistemas estaban asociados con estas identidades. Para cada sistema, se documentaron la seguridad y los datos, que se generaron mediante el MSR.

El estudio del MSR permitió un seguimiento de qué sistemas podrían ser explotados y qué sistema depende de otro. En la Figura 13.7 los sistemas de Alice se organizan de acuerdo con la identidad utilizada. Esto permite determinar una vulnerabilidad en cascada en sistemas que dependen de la seguridad de artefactos de otros sistemas. El propósito de este análisis es modelar la Personalidad de Pluridentidad Digital de Alice como un SoS. A partir de este modelo podemos determinar cuál es el sistema más crítico que podría comprometer cualquier otro,

e identificar fuentes de vulnerabilidades. Este modelo también puede permitirnos enumerar y priorizar las vulnerabilidades existentes en el SoS.

Por ejemplo, podríamos darnos cuenta de que, si Alice pierde su teléfono o su tableta, como consecuencia todos sus DIs están potencialmente comprometidos.

De hecho, los sistemas encontrados en este análisis estaban proporcionando piezas de información sobre ella que nos permitieron llegar a una cuenta de iCloud creada con una identidad de Gmail. La seguridad en este sistema se vio seriamente comprometida. A pesar de que este sistema proporcionaba autenticación de dos factores, Alice no la había activado. En cuanto a la seguridad basada en el conocimiento, iCloud proporciona métodos de recuperación basados en preguntas de seguridad. Esas preguntas son fecha de nacimiento, marca del primer coche, playa favorita, y el destino del primer viaje en avión. Algunas de estas preguntas pueden ser respondidas por los datos publicados por Alice en las redes sociales y otras pueden deducirse razonando sobre los conocimientos adquiridos.

En general, cuando un atacante obtiene acceso a un sistema del DP de Alice, éste podría convertirse en una nueva fuente de datos que podrían ser utilizados en actos maliciosos. Este problema se ha estudiado en otras publicaciones como [41]. Un atacante podría, potencialmente, acceder al teléfono o la tableta de Alice, y descubrir su ubicación precisa, o acceder a documentos y fotos, entre otros, como sucedió en 2014 en "The Fappening".[10]

La forma en que se combinaron los datos de distintas categorías, por lo general procedentes de diferentes sistemas, usados para encontrar datos adicionales, o para generar nuevos datos, se muestra en la Figura 13.8. Esta deducción de datos es similar a la ya realizada por Creese et al. [8]. En su trabajo, los autores desarrollaron una matriz para entender qué datos podrían deducirse según otros datos ya publicados.

Al considerar los perfiles sociales como un Sistema de Sistemas, los datos que se generan de la combinación de distintas fuentes no pertenecen a un sistema único, sino que pertenecen a la Personalidad Digital, es decir, al SoS, ya que se ha generado a partir de un resultado agregado. Empleando la óptica del SoS, la generación de nuevos fragmentos de datos puede considerarse como un comportamiento emergente [27]. La combinación de la información sobre esos sistemas genera un conjunto de datos que no serían accesibles de otra forma.

---

10 https://www.theverge.com/2014/9/2/6099307/celebgate-attack-leaks-nude-photos-of-more-than-100-celebrities

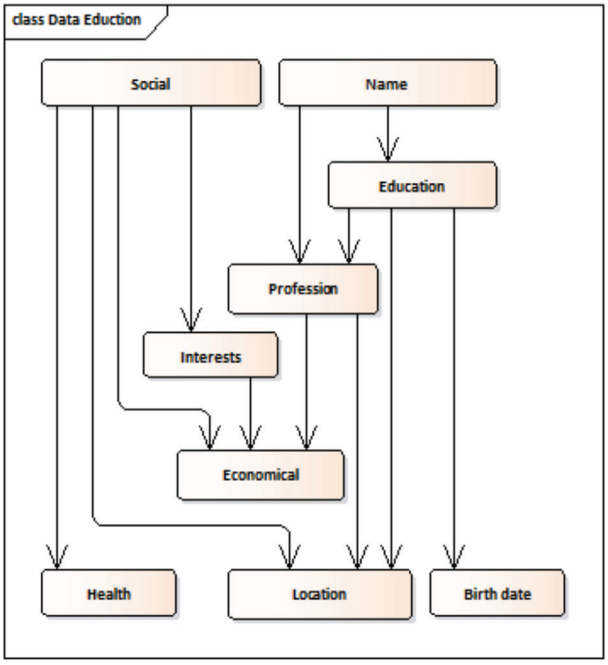

Figura 13.8. Deducción media de datos perso

13.4.3 Análisis de la seguridad de SoS

Después de recopilar los datos de cada sistema de cada sujeto, el análisis del MCPD y MSR nos permite estudiar los datos disponibles y detectar problemas de seguridad entre los diferentes sistemas.

En esta sección se evalúan a los 17 sujetos como si fueran Sistemas de Sistemas, en los que se analiza su seguridad de acuerdo con la capacidad de explotar la seguridad de su SoS mediante el uso de los recursos proporcionados por los sistemas constituyentes.

En cuanto a la seguridad en los sistemas de los sujetos seleccionados, 4 (23%) de ellos han delegado la seguridad de sus identidades a un artefacto, por ejemplo, una memoria USB u otro dispositivo con un software de autenticación; 8 (47%) de ellos a recibir un SMS en sus teléfonos móviles; 13 (76%) confían en recibir un código por correo electrónico utilizando otra identidad digital; y 11 (64%) utilizan una seguridad basada en el conocimiento.

Teniendo en cuenta los datos recopilados, los sujeto #7, #11 y #17 son los DIs mejor protegidos, ya que no pudimos obtener ninguna otra información que nos

ayudara a identificar al individuo. Tampoco se encontraron datos de #2 utilizando las técnicas consideradas en este estudio. Sin embargo, detectamos que los DIs se utilizaron en algunos sistemas y un atacante en un ataque real podría utilizar estrategias más agresivas para permitir una mayor recuperación de datos.

Entre los usuarios que dependen de la seguridad basada en el conocimiento, el más expuesto es el sujeto #6, revelando el nombre completo, la fecha de nacimiento y los datos relevantes de cada categoría. Este DP está utilizando tres identidades, y se detectó un punto débil: una de las identidades puede ser explotada respondiendo al "superhéroe favorito". Al conocer los datos personales de este sujeto, un atacante podría intentar crear una relación cercana y recuperar esta información.

El sujeto #13 está tan expuesto como el #6, pero se considera más seguro ya que los datos revelados no comprometen la seguridad de ninguna identidad. Esta consideración podría cambiar si entra en juego una nueva identidad mediante una seguridad basada en el conocimiento explotable.

Por lo tanto, la PI3 "*¿Podría la sobreexposición convertirse en una vulnerabilidad para la seguridad de las identidades digitales?"* puede ser contestada teniendo en cuenta ambos candidatos. La sobreexposición de un DP puede convertirse en una vulnerabilidad para las identidades digitales si, entre los sistemas utilizados por el DP, cualquiera de ellos está utilizando una seguridad basada en el conocimiento que podría evadirse mediante el uso de datos expuestos.

Por un lado, la seguridad basada en el conocimiento podría ser explotada estableciendo contacto con la víctima. Por otro lado, la seguridad basada en artefactos no es necesariamente una opción más segura. Cuando la autenticación de identidad está basada en artefactos, se debe establecer un mecanismo de seguridad para proteger este nuevo sistema. En este sentido, a menos que haya un bucle de sistemas de seguridad basados en artefactos, la seguridad de los sistemas debe terminar finalmente en un sistema protegido basado en el conocimiento, o peor aún, en un sistema no seguro.

Los conocimientos necesarios para explotar la seguridad de estas personas incluyen responder a: cómo se invitó a Gmail, nombre del perro, primer número de teléfono, nombre completo y fecha de nacimiento, superhéroe favorito, nombre del primer maestro, número de viajero frecuente, código de copia de seguridad de ocho dígitos, cuando se creó la cuenta de Google y el apellido abuela.

La seguridad basada en artefactos más utilizada es recibir un correo electrónico en una bandeja de entrada alternativa. El segundo mecanismo más utilizado para el acceso de recuperación a un sistema se basa en la autenticación de dos factores (2FA). 2FA se puede administrar mediante el uso de aplicaciones exclusivas o mediante la recepción de un SMS que proporciona un código para ser escrito por el usuario. Sin embargo, los teléfonos inteligentes pueden ser robados, y

en algunos casos, las personas no tienen un mecanismo de protección adecuado. En otros casos, se pueden obtener SMS, no obstante, estos mensajes se envían sin un método de cifrado. De esta forma se puede romper el 2FA mediante el *SIM swapping*, en el que los atacantes duplican una tarjeta SIM que les permite recibir cada SMS utilizado para evitar el protocolo 2FA [42].[11]

Este método podría ejecutarse de forma personal para el autoanálisis y determinar los puntos más débiles del DP.

13.4.3.1 AMENAZAS A LA VALIDEZ

Para comprender el contexto y las limitaciones de este estudio enumeramos los factores internos y externos que podrían afectar a los resultados.

La validez interna se refiere a si el resultado del estudio podría venir de otros factores distintos de la sobreexposición de información en SoS. La validez interna puede verse amenazada por la selección de los sujetos y los efectos del estudio en la privacidad del usuario. Los sujetos elegidos eran usuarios activos de un panel de votación en línea español. Entre ellos podríamos reconocer a personas de diferente sexo y edad. Los sujetos también tenían diferentes ocupaciones: estudiantes, empleados públicos, autónomos y profesores. Las personas que utilizaron este panel eran de países de todo el mundo como Argentina, Francia, Italia, México, España o el Reino Unido. La cultura de las personas y su educación podría afectar los resultados de este estudio: tal vez sujetos de distinta cultura podrían ser más cautelosos en la exposición de información sensible. Para mitigar este riesgo, tendríamos que realizar más estudios sobre diferentes conjuntos de usuarios de otras comunidades. Sin embargo, cualquier estudio de este tipo puede afectar la privacidad del usuario, por lo que preferimos no manejar más datos sensibles.

Con respecto a los efectos del estudio, una amenaza a la validez puede derivar de nuestro cuidado extremo en evitar cualquier impacto en los usuarios. Al realizar pruebas más agresivas y descuidadas (como tal vez haría un verdadero atacante) se podrían haber obtenido más datos, pero también afectarían al resultado del estudio. Los candidatos eventualmente podrían obtener un aviso de que sus datos están siendo utilizados o consultados, y así tomar contramedidas que bloquearían el análisis. En cualquier caso, al haber riesgos de exposición optamos por la acción que más salvaguardase la privacidad del sujeto.

Por otro lado, la *validez externa* (es decir, si los resultados pueden generalizarse más allá de los sujetos del estudio y en qué medida) se ve amenazada por el ajuste y la puntualidad. En su conjunto, los candidatos tuvieron una participación

11 https://www.bbc.com/news/business-46047714

digital activa según nuestros hallazgos, sin embargo, no podemos garantizar que este fenómeno ocurra si se replica este estudio con una población diferente. Los sistemas y la seguridad en la vida digital son muy diferentes en cada sujeto. Una vez más, para mitigar este riesgo se necesitarían más estudios.

La puntualidad también es otro factor que afecta a los resultados. Por un lado, a medida que la vida digital en las redes sociales evoluciona muy rápido: si los datos que usamos no fueran recientes, nuestro análisis podría producir resultados que ya no son significativos. Para mitigar este riesgo, usamos una fuga de datos de hace menos de 5 años. A pesar de esto algunas identidades ya estaban obsoletas.

13.5 CONCLUSIONES Y TRABAJO FUTURO

Este estudio describe diferentes métodos y técnicas que un atacante podría utilizar para obtener y combinar datos sobre identidades digitales y cómo estos datos podrían ser explotados mediante el uso de una perspectiva de Sistemas de Sistemas. Los registros de una personalidad de pluridentidad digital se pueden modelar con el Metamodelo de Representación de Personajes Digitales descrito en este estudio. Se han diseñado dos submodelos que facilitan la coincidencia entre los datos recopilados y la seguridad: MCPD y MSR. Estos modelos se pueden utilizar para analizar sistemáticamente la seguridad de los sistemas con respecto a la PD a través de un análisis de representación de personajes de pluridentidad digital. Esto asiste a un estudio sobre la exposición entre diferentes sistemas en los que se usan las identidades de una PD. De esta manera, la seguridad se evalúa en función de cómo una PD se vuelve vulnerable al combinar la información que los sistemas individuales están proporcionando, desde una perspectiva SoS.

El modelo y el método presentados se han utilizado en un estudio para evaluar la seguridad de 17 sujetos anónimos elegidos. El método ARP2D ayudó a organizar los datos recopilados del individuo para analizar y detectar vulnerabilidades que podrían afectar a la seguridad en la PD de los individuos. Esta sobreexposición podría utilizarse para ejecutar ataques de ingeniería social y explotar los sistemas cuya seguridad se basa en el conocimiento.

Nuestro método se puede utilizar de forma ciega, simulando un atacante real que solo puede utilizar la información que encuentra públicamente, o para el autoanálisis, aprovechando el conocimiento completo y haciendo coincidir la información entre diferentes identidades.

Nuestro estudio reveló cómo las pluridentidades nos ponen en riesgo, aunque, por otro lado, los usuarios de internet son cada vez más conscientes sobre la relevancia de la privacidad y sobre el impacto potencial de la publicación de sus datos personales en Internet. Por lo tanto, para concluir con una observación

positiva, podemos decir que cuantos más conscientes se vuelvan las personas, más difícil será encontrar evidencias de inseguridades en la vida digital mediante el uso de este método.

Este estudio forma parte del trabajo en curso TeSSoS [37], que describe cinco etapas para evaluar la seguridad en el contexto SoS. TeSSoS comienza con la etapa *SoS Discovery* para definir el ámbito del SoS. A continuación, las vulnerabilidades se revelan durante la etapa Requisitos *rojos* y las contramedidas de las vulnerabilidades se definen en la de Requisitos *azules*. La implementación de seguridad se centra en el desarrollo y la formación. Por último, las contramedidas se evalúan y validan intentando aprovechar las vulnerabilidades definidas anteriormente.

Las dos primeras etapas de TeSSoS se implementan en este estudio: Digital Persona Portrayal implementando el *SoS Discovery* y ARP2D como Requisitos *Rojos*. Las tres etapas restantes de validación se consideran trabajos futuros, así como la implementación de TeSSoS en otras arquitecturas SoS.

Además, se programan tres trabajos de validación. El primero se basa en la aplicación de métodos de juicio de expertos a los problemas relacionados con el modelado, la seguridad y las pruebas mediante el uso del método Delphi [10].

A continuación, se pretende realizar una validación industrial de este enfoque en colaboración con algunas empresas estudiando la exposición de sus empleados utilizando este enfoque y evaluar si la sobreexposición pudiese convertirse en una vulnerabilidad no sólo para los empleados, sino también para la organización interpretada como un SoS en el que los empleados son considerados como sistemas constituyentes. De esta manera, el equipo de seguridad de la empresa puede establecer algunas métricas sobre cuán expuestos están los empleados y ajustar los privilegios de cada individuo o diseñar estrategias defensivas.

Una tercera validación consideraría el estudio de viabilidad de desarrollar contramedidas de algunas vulnerabilidades definidas como requisitos azules en los sistemas constituyentes que lo permitiesen.

Este tipo de validaciones han sido realizadas previamente por coautores con resultados satisfactorios como en [49] [14].

El trabajo futuro descrito incluye probar este método simulando ataques reales. Por ejemplo, las empresas pueden utilizar este enfoque para evaluar el nivel de exposición de sus empleados. No obstante, la validación puede verse amenazada debido a consideraciones éticas. Por un lado, los posibles ataques deben ser permitidos por los candidatos antes de ser lanzados, por otro lado, los candidatos no serían informados antes del ataque, porque esto puede afectar a sus reacciones si se produce una interacción, produciendo resultados inexactos [26] [5].

Id	Demografía & Identificador	Ubicación	Profesor	Educación	Económico	Social	Salud	Intereses
1	3 identidades, 8 sistemas Nombre completo	Y	Y	Y	N	N	N	N
2	3 identidades, 4 sistemas Nombre completo	N	N	N	N	N	N	N
3	2 identidades, 3 sistemas Nombre parcial	P	N	Y	N	N	N	N
4	2 identidades, 4 sistemas Nombre completo, Fecha de nacimiento parcial	Y	Y	Y	P	N	N	N
5	2 identidades, 4 sistemas Nombre completo, Fecha de nacimiento parcial	Y	Y	N	P	Y	N	Y
6	3 identidades, 10 sistemas Nombre completo, Fecha de nacimiento parcial	Y	Y	Y	Y	Y	N	Y
7	3 identidades, 3 sistemas	N	N	N	N	N	N	N
8	1 identidad, 1 sistema	Y	Y	N	N	N	N	N
9	3 identidades, 8 sistemas Nombre completo	Y	Y	N	Y	N	N	Y
10	3 identidades, 4 sistemas Nombre completo	N	N	N	N	N	N	Y
11	1 identidad	N	N	N	N	N	N	N
12	3 identidades, 4 sistemas Nombre parcial	Y	N	N	N	N	N	N
13	3 identidades, 10 sistemas Nombre completo, Fecha de nacimiento parcial	Y	Y	Y	Y	Y	N	Y
14	2 identidades, 3 sistemas Nombre parcial	P	N	N	N	N	N	Y
15	1 identidad, 7 sistemas Nombre completo	Y	Y	N	N	N	N	P
16	2 identidades, 5 sistemas Nombre parcial	Y	N	N	N	N	N	N
17	3 identidades, 3 sistemas	N	N	N	N	N	N	N
T	40 identidades, 82 sistemas	10 Y 58%	8 Y 50%	5 Y 30%	3 Y 17%	3 Y 17%	-	6 Y 35%

Tabla 13.2. Resultados del análisis manual de 17 candidatos. PARTE I

Id	Proveedor de Identidad	Artefactos	Conocimiento
1	Gmail x1 Hotmail x1	Otra bandeja de entrada Número de teléfono	¿Quién te invitó a Gmail?
2	Gmail x1 Hotmail x1	Otra bandeja de entrada Número de teléfono	Nombre del perro
3	Gmail x2	Otra bandeja de entrada	¿Cuándo se creó la cuenta de Gmail?
4	Hotmail x1 Correo electrónico de trabajo x1	Otra bandeja de entrada	--
5	Teléfono x1 Gmail x1	Otra bandeja de entrada Número de teléfono	Número de identificación nacional Nombre Fecha de nacimiento
6	Gmail x2 Correo electrónico de trabajo x1	Número de teléfono Tableta Otra bandeja de entrada	Superhéroe favorito
7	Hotmail x2 Gmail x1	Otra bandeja de entrada	¿Hasta dónde quieres llegar hoy?
8	Correo electrónico de trabajo	--	--
9	Gmail x2 Correo electrónico de trabajo x1 Hotmail x1	Número de teléfono Otra bandeja de entrada	Nombre del primer maestro
10	Gmail x2 Hotmail x1	Número de teléfono Otra bandeja de entrada	Código de copia de seguridad Número de viajero frecuente
11	LA IDENTIDAD YA NO EXISTE		
12	Gmail Hotmail x2	Número de teléfono Dispositivo telefónico Otra bandeja de entrada	Nombre del primer maestro
13	Hotmail Gmail Yahoo	-	--
14	Hotmail Gmail x2	Dispositivo telefónico Otra bandeja de entrada	Nombre del primer maestro
15	Gmail	Memoria USB	--
16	Gmail Outlook	Número de teléfono Dispositivo telefónico	Apellido de abuela
17	Hotmail x3	Otra bandeja de entrada	--
T	--		

Tabla 13.3. Resultados del análisis manual de 17 candidatos. PARTE II

13.6 REFERENCIAS

[1] Abass IAM. "Social Engineering Threat and Defense: A Literature Survey." *J. Inf. Secur.* 2018. Vol. 09, No. 04, pp. 257–264.

[2] Aktypi A, Nurse JRC, and Goldsmith M, "Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and Online Social Networks," in *MPS 2017 - Proceedings of the 2017 Workshop on Multimedia Privacy and Security, co-located with CCS 2017*, 2017.

[3] Antonius N, and Rich L, "Discovering collection and analysis techniques for social media to improve public safety," *Int. Technol. Manag. Rev.*, 2013.

[4] Atote BS, Zahoor S, Dangra B, Bedekar M. "Personalization in user profiling: Privacy and security issues", *Int. Conf. on Internet of Things and Applications IOTA,* Pune, 2016, pp. 415-417.

[5] Carpenter S, Zhu F, and Kolimi S, "Reducing online identity disclosure using warnings," *Appl. Ergon.*, 2014.

[6] Clarke R, "The digital persona and its application to data surveillance." *The Information Society*, Vol. 10, No. 2, pp. 77-92, online at http://www.rogerclarke.com/DV/DigPersona.html#DP, 1994. (último acceso mayo 2021).

[7] Clarke R, http://www.rogerclarke.com/ID/IdModel-Gloss-1002.html, 2010. (último acceso mayo 2021).

[8] Creese S, Goldsmith M, Nurse JRC, and Phillips E, "A data-reachability model for elucidating privacy and security risks related to the use of online social networks," in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012.

[9] Dahmann JS, Baldwin KJ. "Understanding the current state of US defense systems of systems and the implications for systems engineering." *IEEE Int. Syst. Conf. Proceedings, SysCon.* 2008, pp. 99–105.

[10] Dalkey N, Helmer O. "An Experimental Application of the Delphi Method to the use of experts." *Management Science. 9 (3).* 1963, pp. 458–467. doi: https://doi.org/10.1287%2Fmnsc.9.3.458

[11] Di Martino M, Robyns P, Weyts W, Quax P, Lamotte W, & Andries K. "Personal Information Leakage by Abusing the GDPR 'Right of Access'". In Fifteenth Symposium on Usable Privacy and Security, 2019.

[12] El-Maliki T, Seigneur JM, "User-centric Mobile Identity Management Services." *Int. Conf. Emerg. Secur. Information, Syst. Technol.* 2007. pp. 33–76.

[13] Emanuel L, Bevan C, and Hodges D, "What Does Your Profile Really Say About You?: Privacy Warning Systems and Self-disclosure in Online Social Network Spaces," in *Conference on Human Factors in Computing Systems - Proceedings*, 2013.

[14] Escalona MJ, López G, Vegas S, et. Al. "A Software Engineering Experiments to value MDE in testing. Learning Lessons." *XXI JISBD*. 2016.

[15] Foozy C, Ahmad R, Abdollah M, "Generic Taxonomy of Social Engineering Attack." *Malaysian Tech. Univ. Int. Conf. Eng. Technol. MUiCET*. 2011. No. MUiCET, pp. 527–533.

[16] Garfinkel SL, "Email-based identification and authentication: An alternative to PKI?," *IEEE Security and Privacy*. 2003.

[17] Gross R, Acquisti A, and Heinz H. J., "Information revelation and privacy in online social networks," in *WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 2005.

[18] Gupta P, Gottipati S, Jiang J, and Gao D, "Your love is public now: Questioning the use of personal information in authentication," in *ASIA CCS 2013 - Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, 2013.

[19] HaveIBeenPwned. https://haveibeenpwned.com/ (accessed January 2020)

[20] How to get started in online investigations with open-source intelligence. Medium. https://medium.com/1st-draft/how-to-get-started-in-online-investigations-with-open-source-intelligence-71d0ddc0f639 2016. (último acceso mayo 2021)

[21] Hodges D, Creese S, and Goldsmith M, "A model for identity in the cyber and natural universes," in *Proceedings - 2012 European Intelligence and Security Informatics Conference, EISIC 2012*, 2012.

[22] Hutchings A, Pastrana S. Understanding eWhoring. 2019. arXiv preprint arXiv:1905.04576.

[23] Identity Leak Checker. Hasso-Plattner-Institut https://sec.hpi.de/ilc/

[24] ISO/IEC IS 21839:2019: Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system. International Organization for Standardization, Geneva, Switzerland.

[25] Jagatic TN, Johnson NA, Jakobsson M, Menczer F. "Social phishing." *Commun. ACM.* 2007. Vol. 50. No. 10, pp. 94–100.

[26] Krasnova H, Günther O , Spiekermann S, and Koroleva K, "Privacy concerns and identity in online social networks," *Identity Inf. Soc.*, 2009.

[27] Maier MW, "Architecting principles for systems-of-systems," *Syst. Eng.*, 1998.

[28] Malhotra A, Totti L, Meira W, Kumaraguru P, and Almeida V, "Studying user footprints in different online social networks," in *Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012*, 2012.

[29] Mansour RF. Understanding how big data leads to social networking vulnerability. Comput. Human Behav. 2016. Vol. 57, pp. 348–351.

[30] My data request. https://mydatarequest.com/ (último acceso mayo 2021).

[31] Minkus T, Ding Y, Dey R, and Ross KW, "The city privacy attack: Combining social media and public records for detailed profiles of adults and children," in *COSN 2015 - Proceedings of the 2015 ACM Conference on Online Social Networks*, 2015.

[32] Mitnick KD, Simon WL. "The art of deception: controlling the human element of security," *W. Publishing., Ed. Indianapolis: Wiley Publishing,* 2002.

[33] Mouton F, Malan MM, Leenen L, Venter HS. "Social engineering attack framework." *Inf. Secur. South Africa - Proc. ISSA*. 2014 Conf., pp. 1–9.

[34] Mueller ML, Park Y, Lee J, Kim TY. "Digital identity: How users value the attributes of online identifiers." *Inf. Econ. Policy.* 2006. Vol. 18, No. 4, pp. 405–422.

[35] Nurse JRC, Erola A, Gibson-Robinson T, Goldsmith M, and Creese S, "Analytics for characterising and measuring the naturalness of online personae," *Secur. Inform.*, 2016.

[36] Olivero MA, Bertolino A, Dominguez-Mayo FJ, Escalona MJ, and Matteucci I, "Addressing Security Properties in Systems of Systems: Challenges and Ideas," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019.

[37] Olivero MA, Bertolino A, Dominguez-Mayo FJ, Escalona MJ, Matteucci I. "Security Assessment of Systems of Systems." *SESoS.* 2019.

[38] OMG, OMG Unified Modeling Language, v2.5. http://www.omg.org/spec/UML/, 2015 (último acceso mayo 2021).

[39] Perito D, Castelluccia C, Kaafar MA, and Manils P, "How unique and traceable are usernames?," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2011.

[40] Qiu L, Lu J, Yang S, Qu W, and Zhu T, "What does your selfie say about you?," *Comput. Human Behav.*, 2015.

[41] Rabkin A, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," in *SOUPS 2008 - Proceedings of the 4th Symposium on Usable Privacy and Security*, 2008.

[42] Reese K, Smith T, Dutson J, Armknecht J, Cameron J, and Seamons K, "A Usability Study of Five Two-Factor Authentication Methods," in *Proc. the 15th Symposium On Usable Privacy and Security (SOUPS)*, 2019.

[43] Salahdine F, Kaabouch N. "Social Engineering Attacks: A Survey." *Futur. Internet.* 2019. vol. 11, no. 4, p. 89.

[44] Shirey, R. W. Internet security glossary, version 2. https://tools.ietf.org/pdf/rfc4949.pdf 2007 (último acceso mayo 2021).

[45] Spiderfoot. https://www.spiderfoot.net/documentation/#what-is-spiderfoot/ 2019 (último acceso mayo 2021).

[46] Tajbakhsh M, Homayounvala E, Shokouhyar S. "Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage." *Int. J. Electron. Secur. Digit. Forensics.* 2017. Vol. 9, No. 1, p. 62.

[47] Torrecilla CJ, Escalona MJ, Mejías M. "A Delphi-based expert judgment method applied to the validation of a mature Agile framework for Web development projects." *IT&M* 2018. 1-32. https://doi.org/10.1007/s10799-018-0290-7

[48] European Union. General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 2016. (último acceso mayo 2021)

[49] Urbieta M, Escalona MJ, Rossi G, Robles-Luna E. "Detecting Conflicts and Inconsistencies. Web Application Requirements." *Lecture Notes in Computer Science.* 2012. Vol. 1. 7959. 278-288. DOI: 10.1007/978-3-642-27997-3_27

[50] Wayman JL. "Biometrics in identity management systems. Security & Privacy." *IEEE*. 2008. Vol. 6, No. 2, pp.30–37.

[51] Zheqiang-Gong N, Liu B. "You are Who You Know and How You Behave: Attribute Inference Attacks via Users' Social Friends and Behaviors" in *SEC16 – Proceedings of the 25th USENIX Conference on Security Symposium*, 2016.