Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo digital de proximidad: *Análisis preliminar de riesgos*

Gustavo Betarte[*§], Juan Diego Campo[*§], Andrea Delgado[*§], Pablo Ezzatti[*§], Álvaro Forteza[†], Laura González[*§], Álvaro Martín[*§], Bárbara Muracciole[‡], Raúl Ruggia[*§]

[*]Instituto de Computación, Facultad de Ingeniería, Universidad de la República

[†]Departamento de Economía, Facultad de Ciencias Sociales, Universidad de la República

[‡]Centro de Derecho Informático, Facultad de Derecho, Universidad de la República

[§]Área Informática, PEDECIBA

3 de junio de 2020

***Resumen*—La utilidad de una aplicación de rastreo digital de proximidad (RDP) radica en su capacidad para detectar contactos en riesgo y utilizar esta información en conjunto con otras medidas para combatir la epidemia, como la realización de tests, el distanciamiento social o la cuarentena. En el contexto del proyecto PROTECT [1] se ha trabajado en identificar las propuestas existentes, las tecnologías, flujos de datos y procesos involucrados en el funcionamiento de sistemas RDP. Actualmente está instalado a nivel internacional un interesante debate entre especialistas en el campo de la seguridad y la protección de datos personales, en el marco de las distintas opciones planteadas. Este documento presenta los resultados de realizar un análisis preliminar de seguridad y privacidad de soluciones de RDP y los diferentes modelos definidos. Uruguay planea desplegar una solución tecnológica, usando una aplicación móvil, destinada a notificar a los usuarios si han estado en contacto con una persona diagnosticada con COVID-19. Se estipula que la aplicación se comportará de forma tal que la seguridad de los datos que manipula así como la privacidad de sus usuarios serán garantizadas. Con este trabajo se intenta contribuir al debate público aportando a definir con precisión, con la mirada puesta en la seguridad y la privacidad de las personas, lo que una aplicación de RDP podría, o no, garantizar.**

***Index Terms*—COVID-19, rastreo digital de proximidad, soluciones tecnológicas, protección de datos personales, seguridad informática, análisis de riesgo.**

I. Introducción

La utilidad de una aplicación de rastreo digital de proximidad (RDP) en el contexto de una epidemia, radica en su capacidad para detectar contactos en riesgo de contagio y utilizar esta información para combatirla, en conjunto con otras medidas como la realización de tests, el distanciamiento social o la cuarentena.

Este trabajo es parte del proyecto PROTECT que cuenta con apoyo del Programa *Conocimiento especializado para enfrentar la emergencia planteada por el COVID19 y sus impactos* de la Comisión Sectorial de Investigación Científica (CSIC), Universidad de la República (UdelaR), Uruguay.

Este documento presenta los resultados de realizar un análisis preliminar de seguridad y privacidad de soluciones de RDP. En el contexto del proyecto PROTECT se ha trabajado en identificar precisamente las tecnologías, flujos de datos y procesos involucrados en el funcionamiento de sistemas RDP. Hemos consolidado, además, un catálogo de las amenazas y riesgos inherentes a las soluciones de RDP que han sido identificados por expertos en el área y publicados en trabajos muy recientes.

Actualmente está instalado a nivel internacional un interesante debate entre especialistas en el campo de la seguridad y la protección de datos personales a menudo enfrentando las aplicaciones llamadas *descentralizadas*, siguiendo un enfoque cuya propuesta ha sido liderada por el consorcio DP-3T [2], y las *centralizadas*, que es el que proponen los equipos diseñadores del protocolo ROBERT [3] e implementado en la aplicación StopCovid de Francia [4]. Recientemente las empresas tecnológicas Apple y Google anunciaron [5] un esfuerzo conjunto para combatir la pandemia de COVID-19 desarrollando una tecnología de rastreo de contactos para ayudar a los gobiernos y las agencias de salud a reducir la propagación del virus, tomando como criterio central, según sus declaraciones, la privacidad y seguridad del usuario. El anuncio de la asociación incluyó especificaciones técnicas de la tecnología planificada, que tiene un gran potencial para una adopción generalizada debido al alcance global de las dos compañías. Esta tecnología, provista como una API (*Application Programming Interface*) provee soporte técnico solamente para soluciones RDP descentralizadas.

En este contexto, Uruguay planea desplegar una solución RDP para ayudar a combatir la expansión de COVID-19, y se estipula que garantizará la seguridad de los datos que manipula así como la privacidad de sus usuarios. La solución estará implementada a través de una aplicación móvil, apoyada en la API provista por Apple y Google, por lo cual seguirá un

enfoque descentralizado.

Los enfoques descentralizado y centralizado en general, así como uno de los principales representantes de cada uno, DP-3T y ROBERT, respectivamente, se presentan en la sección III. Sin embargo, en este trabajo no solo intentaremos describir los dos enfoques mencionados y los posibles riesgos que traen aparejados, si no que además discutiremos los posibles abusos a los que se puede ver expuesta una solución de RDP, independientemente del protocolo adoptado. Este es el tema que se trata en la sección II. También hemos incorporando en nuestro análisis las restricciones tecnológicas y marco regulatorio propios de nuestro país.

Es nuestra visión que un análisis de riesgos de una solución de RDP tiene que incluir todos los componentes del sistema que instrumentan su operativa. Aún cuando esté inspirada en los modelos hegemónicos referidos, toda implementación nacional de solución de RDP necesariamente incorporará sus propias decisiones y características socio-biológicas, así como tecnológicas y normativas.

Nuestro equipo de investigación no cuenta con la información necesaria para realizar un análisis completo de lo que se está pensando sea la solución uruguaya de RDP, sin embargo entendemos que el presente análisis contempla componentes y características funcionales que seguramente estarán presentes en una solución tal. En este sentido, en la sección IV presentamos un análisis preliminar de riesgos asociados específicamente a los enfoques descentralizados, en particular DP-3T, y centralizados, en particular ROBERT.

Finalmente, a modo de conclusión, en la sección V se realiza una consideración en relación a los principios de seguridad y privacidad que entendemos deberían guiar un análisis de riesgos adecuado para evaluar la pertinencia y eventualmente definir un sistema de RDP.

II. Consideraciones generales

Todas las tecnologías de RDP que estudiamos en este trabajo están basadas en el uso de la tecnología Bluetooth, más precisamente *Bluetooth Low Energy (BLE)*, y siguen un patrón de rastreo similar, que describimos a continuación:

1. cada dispositivo móvil participante transmite constantemente, a través de sus dispositivos de comunicación de corto alcance, un número aleatorio (identificador efímero) que cambia cada pocos minutos; simultáneamente, cada dispositivo registra los identificadores recibidos de los dispositivos vecinos,
2. tan pronto como el propietario de un dispositivo es notificado que ha sido diagnosticado positivo y fue potencialmente contagioso durante un cierto período de tiempo, se carga con su consentimiento los identificadores que su dispositivo transmitió (o recibió) durante ese período de tiempo en un registro,
3. haciendo uso de ese registro es posible verificar si un usuario estuvo en contacto con una persona infectada. Si se determina que hubo un contacto, el propietario es notificado de que estuvo expuesto al virus y de los pasos que debe seguir (solicitar un test, mantenerse en cuarentena, o lo que la autoridad sanitaria considere adecuado según el caso).

Si bien las distintas propuestas difieren en varios aspectos como la generación de los identificadores o el lugar donde ser realiza el cálculo del riesgo de exposición, alcanza con esta descripción de alto nivel para identificar riesgos de privacidad inherentes a todas las soluciones de este tipo. Numerosos investigadores del dominio de la criptografía, la seguridad informática y del derecho informático, entre ellos los autores de DP3T y ROBERT, han publicado en los meses de abril y mayo de 2020 reportes que presentan análisis de seguridad y privacidad de soluciones RDP [6, 7, 8].

Como un resultado inicial de nuestra investigación hemos consolidado un catálogo de las amenazas y riesgos más relevantes que han sido identificados por estos trabajos, los cuales se describen en las subsecciones siguientes. Es importante notar que la mayoría de estos riesgos son completamente independientes de los detalles de la aplicación particular y en muchos casos no requieren ninguna habilidad informática particular. Estos riesgos se resumen en el cuadro I, utilizando la categorización definida en [6]: riesgos inherentes (RI) de sistemas de rastreo de proximidad, riesgos específicos (RE) de cualquier sistema que registra identificadores recibidos por BLE, riesgos generales (RG) de cualquier sistema de rastreo de proximidad que usa BLE, y riesgos originados por el uso de sistemas de red (RR).

II-A. Certificación de pacientes COVID-19 positivos

La primera consideración es que debe existir un mecanismo que certifique que un usuario efectivamente padece la enfermedad. De otro modo, si las personas tienen la capacidad de comunicar al sistema que son portadores del virus pero esta afirmación no es verificada adecuadamente, estaríamos ante la presencia de un potencial uso abusivo del sistema, que podría generar, entre otras cosas, falsos positivos. Este tipo de comportamientos le quitarían credibilidad a la solución y desestimularían su adopción.

Es por esto que la enfermedad de la persona debe ser confirmada por una prueba o un profesional médico para que el sistema acepte difundir su información. Si bien la mayoría de las soluciones estudiadas prevén la utilización de este tipo de mecanismos, éstos generalmente no son especificados en detalle y su definición se deja en manos de la implementación que se realice en cada país.

Cualquiera sea el mecanismo, un atacante puede encontrar formas de ingresar en el sistema como infectado. Estas son las mencionadas en [6]:

- estar efectivamente infectado o infectarse posteriormente a haber realizado un ataque.
- pagarle a una persona que presenta síntomas y sospecha estar infectada para que lleve al hospital el celular del atacante en lugar del propio al ir a realizarse el test.
- ingresar de manera no autorizada a los sistemas de la autoridad sanitaria o sobornar a un funcionario para recibir un certificado de infección.

II-B. Anonimato de los datos

Para poder advertirle a un usuario de la aplicación que ha estado en contacto con una persona infectada, es necesario

Riesgo	Impacto	Descripción
RI 1	Identificar usuarios infectados	Es posible para un atacante obtener la identidad de personas infectadas combinando la siguiente información: 1) con quién interactúa en cada momento (se obtiene por fuera de la aplicación) y 2) el hecho de haber estado en contacto con una persona infectada en un momento específico (se obtiene de la aplicación). Ver sección II-C
RI 2	Prevenir notificaciones	Es posible para un atacante evitar que (algunos) usuarios sean notificados de que estuvieron en riesgo de exposición, aunque sí hayan estado expuestos. Para esto, simplemente decide no participar en el rastreo de proximidad, desactiva la aplicación temporalmente (o el bluetooth) o no envía los datos de proximidad registrados en la aplicación aunque haya sido diagnosticado como positivo.
RI 3	Falsear riesgos de exposición	Es posible para un atacante ingresar falsamente en el sistema como infectado, provocando, por ejemplo, que otros usuarios reciban falsas alarmas. Ver sección II-A.
RE 1	Revelar interacciones sociales	Si se tiene acceso a la cantidad de Ids que fueron registrados en una determinada ventana de tiempo por un dispositivo, es posible estimar la cantidad de personas con que se estuvo en contacto durante ese tiempo. Si se tiene acceso a los Ids registrados por un dispositivo, es posible confirmar que se estuvo en contacto con una tercera parte si se conoce un Id emitido por ella durante el contacto. Ver sección II-F.
RE 2	Recomputar el riesgo de exposición	Si se tiene acceso a la información registrada localmente en un dispositivo, es posible usarla para recomputar el riego de exposición, potencialmente sin consentimiento, lo cual puede llevar a discriminación contra individuos. Ver sección II-F.
RG 1	Causar falsas alarmas mediante extensiones de rango de BLE	Es posible para un atacante conectar su dispositivo a una antena y/o transmisor potente para incrementar el rango de alcance de BLE, logrando que dispositivos lejanos lo registren como próximo. Luego debe reportarse como positivo (ver sección II-A) para asegurarse de que estas interacciones sean marcadas como exposiciones en riesgo. Ver sección II-D.
RG 2	Causar falsas alarmas mediante ataques de retransmisión (relay attacks)	Es posible para un atacante retransmitir señales BLE de personas que tienen alta probabilidad de ser diagnosticadas positivas, por ejemplo de quienes están en un centro de testeo. Ver sección II-D.
RG 3	Identificar ubicaciones con personas infectadas presentes / geolocalización	Es posible para un atacante identificar por ejemplo viviendas de personas infectadas (similar a RI 1) caminando o circulando en algún vehículo por una zona de interés, para asociar ubicaciones (casas) con personas infectadas (ver sección II-C). También existe el riesgo de que se aproveche un sistema RDP para hacer un seguimiento geográfico aproximado de usuarios infectados (ver sección II-E).
RG 4	Interrumpir descubrimiento de contactos	Es posible para un atacante con un bloqueador de bluetooth (bluetooth jammer) interrumpir la comunicaicón entre usuarios del sistema, impidiendo que los contactos de proximidad puedan ser establecidos. Ver sección II-G.
RG 5	Rastrear un dispositivo con bluetooth activado	La activación de bluetooth tiene riesgos como: 1- el dispositivo sea rastreable si el sistema operativo no implementa aleatorización de dirección MAC y desactiva anuncios; 2- mala sincronización entre la aleatorización de dirección de MAC y los identificadores bluetooth hacen al dispositivo rastreable mientras el atacante se mantenga en rango. El punto 1 está resuelto en la mayoría de los sistemas operativos; el punto 2 sería resuelto con la propuesta de Apple/Google. Ver sección II-G.
RG 6	Revelar uso (o no uso) de la aplicación de rastreo	La activación de bluetooth y transmisión de identificadores específicos revela a cualquier observador (por ejemplo un atacante) que la aplicación de rastreo está instalada. Esto no sería particularmente sensible, al ser visto como contribución al bien social en muchas sociedades, pero también revelaría el hecho de que la aplicación no se está usando. Ver sección II-G.
RR 1	Identificar usuarios infectados a través de identificador de red	Si los datos de usuarios con diagnóstico positivo se suben directamente desde su dispositivo móvil, la identidad del usuario queda expuesta a un administrador de sistema o servidor central. Se puede mitigar mediante un proxy, ej. un hospital [6, pp 10]. Ver sección II-C.
RR 2	Identificar usuarios infectados a través de análisis de tráfico de red	Si los datos de usuarios con diagnóstico positivo se suben directamente desde su dispositivo móvil, es posible detectar que se suben datos al servidor e inferir que se trata de alguien con diagnóstico positivo. Se puede mitigar usando encriptación y haciendo que usuarios sanos suban datos vacíos que son descartados por el servidor [6, pp 10]. Ver sección II-C.

Cuadro I
RIESGOS INHERENTES, ESPECÍFICOS Y GENERALES DE SOLUCIONES RDP.

que el sistema maneje algún tipo de registro con datos de los usuarios. Por ejemplo, podría mantener una base de datos con los nombres e información de contacto de esas personas. Esta idea ha sido descartada desde el inicio por los creadores de los protocolos analizados, por no satisfacer propiedades básicas de privacidad. En su lugar, el registro contiene los identificadores efímeros de los usuarios (que pueden ser los transmitidos por las personas infectadas o los recibidos por ellas, según el tipo de solución), o alguna clave que permite reconstruirlos.

Estos registros están *seudonimizados*, lo que significa que los pacientes no están identificados por su nombre o algún otro identificador único, sino por un código o un número que es independiente de su identidad real. En los sistemas propuestos, los registros de pacientes con COVID-19 están seudonimizados con mecanismos criptográficos. Sin embargo, este número podría ser de-anonimizado combinándolo con otra información en la base de datos (los identificadores de las personas que han estado en contacto), o fuera de la base de datos (por ejemplo, recopilada con una antena Bluetooth), o por uso de direcciones IP. No se trata, por lo tanto, de registros completamente anónimos.

Ciertos marcos jurídicos, tales como el Reglamento General de Protección de Datos de la Unión Europea (GDPR), entienden que los datos personales que hayan sido sometidos a seudonimización, que podrían atribuirse a una persona física mediante el uso de información adicional, deben considerarse como información sobre una persona física identificable. Así lo dispone el citado Reglamento en su Considerando 26. Esto significa que una base de datos seudonimizados contiene datos personales y por tanto debe aplicársele las normas rectoras en la materia, no así en caso de tratarse de información anonimizada. La Unidad Reguladora y de Control de Datos Personales ha recogido el citado criterio en forma expresa en la Resolución Nº 68/2017 de 26 de abril de 2017, mediante la cual aprueba los Criterios de Disociación de Datos Personales. En este sentido ha manifestado que el tratamiento de datos que opte por utilizar técnicas de seudonimización, no queda excluido de la aplicación de las normas sobre protección de datos personales, como sí quedarían procesos de disociación o de anonimización de los datos. Es corriente la confusión entre los términos seudonimización, disociación y anonimización. No obstante, desde el punto de vista jurídico poseen significados y consecuencias distintos. Identificar con claridad el proceso técnico utilizado por las tecnologías en estudio es determinante para saber cuál será el régimen jurídico aplicable y valorar su cumplimiento por el responsable del tratamiento de la información. En esta hipótesis, además, estamos ante datos de salud, sensibles y especialmente protegidos por nuestra ley, cuyo tratamiento se encuentra fuertemente restringido, sujeto al previo, expreso y escrito consentimiento informado, o amparado en ciertas excepciones tasadas. Debido a lo cual, la ley exige fuertes medidas de seguridad. Al respecto ¿podemos afirmar que la seudonimización de datos constituye una fuerte medida de seguridad? No, al menos desde el punto de vista jurídico.

II-C. Identificación de personas infectadas

Aunque los seudónimos de los pacientes no revelan directamente sus identidades, los usuarios pueden en algunos casos inferir información sobre otros usuarios tan pronto como se enteran de que una persona a la que han estado próximos físicamente en las últimas dos semanas se ha enfermado. Es importante resaltar que no es necesario que un usuario tenga certeza absoluta de la identidad de una persona infectada para que se den potenciales problemas. En efecto, alcanza con que un usuario malintencionado tenga una fuerte sospecha (fundada o no) para que tome acciones como divulgar la identidad del infectado entre sus conocidos o en redes sociales.

Dos simples escenarios (2 y 3), discutidos en [8] ilustran las limitaciones inherentes a este tipo de sistema. En el primero, una persona que sólo sale de su casa para ir al almacén recibe una notificación de exposición, el usuario concluye (quizás erróneamente) que el almacenero está infectado. En el segundo una persona recibe una notificación y empieza a averiguar con conocidos y compañeros de trabajo quién puede ser el paciente. A partir de estas averiguaciones concluye (quizás erróneamente) que se trata de un vecino médico y que éste infectó a todo el barrio.

Todos los sistemas de RDP pueden además revelar si una persona en particular resulta infectada. Para obtener información sobre una persona específica podemos usar un teléfono en el que instalamos la aplicación y que solamente lo usamos cuando estamos en contacto con esta persona. El teléfono registrará el contacto, y si la persona es diagnosticada positiva, nuestro teléfono recibirá una alerta. A los efectos de ilustrar este tipo de abuso del sistema, en [8] se presenta el siguiente ejemplo. Una compañía tiene la intención de reclutar a un empleado temporal. Quieren asegurarse de que el candidato no se enferme entre la entrevista de trabajo y la firma del contrato. Por lo tanto, usan un teléfono dedicado que se enciende solo durante la entrevista y que recibirá una alerta si el candidato luego da positivo por la enfermedad.

Algunos ataques un poco más sofisticados reportados (aplicables principalmente en esquemas descentralizados) consisten en ubicar un receptor bluetooth junto con una cámara de video en un lugar muy concurrido, registrando al mismo tiempo el identificador bluetooth y la imagen de la persona [7]; comercios que abusan de clientes que instalan su aplicación de compras online para cruzar datos con la información de RDP (escenario 13 en [8]); malware que es instalado en los dispositivos de los usuarios (escenario 14), entre otros.

Además de identificar a usuarios infectados, usando la misma idea también es posible identificar lugares habitados o frecuentados por personas infectadas [6]. Para ello un atacante transita por una zona de su interés, idealmente en un horario de poca circulación, registrando los identificadores que recibe por BLE y asociándolos a lugares físicos específicos. Cuando el atacante recibe una notificación de riesgo de contagio, puede asociar esta notificación a un lugar en particular.

Finalmente, existe una clase de riesgos relacionados al uso de redes de comunicación para trasmitir información sensible. Todo sistema de RDP en el que individuos infectados suben datos a un servidor central desde su dispositivo, potencialmen-

te puede revelar, tanto a un administrador del servidor central como a un observador con capacidades de monitorear el tráfico hacia el servidor, el estado sanitario del individuo.

II-D. Generación de falsas alarmas

En todos los sistemas propuestos es posible generar falsas alarmas en el sistema de modo que usuarios que no están en riesgo reciban una alerta de contacto.

Una posibilidad, descrita en [6], es que un usuario malintencionado extienda el alcance de los dispositivos con antenas bluetooth potentes. Con este método puede diseminar sus propios identificadores en grandes áreas (lo que generará gran cantidad de falsos positivos si está infectado o logra que el sistema lo registre como tal (ver sección II-A)). También es posible retransmitir los identificadores de personas que se sospecha puedan ser positivos, por ejemplo los que entran a un laboratorio donde se realiza el test.

En [8] se describen otros escenarios que requieren menos habilidad técnica por parte del atacante. Es posible, por ejemplo, que un usuario que sospecha estar infectado sea sobornado, forzado, o simplemente venda el servicio de darle su celular a un usuario malicioso, que luego lo utiliza para generar falsos positivos. Puede recorrer con este celular lugares públicos muy concurridos (generando gran cantidad de falsos positivos), o lugares específicos obteniendo algún beneficio particular (por ejemplo, generando una alerta en un competidor deportivo, en otro aspirante a un cargo en una entrevista de trabajo, en toda una clase para que se cancele un examen, etc.). También lo puede utilizar para ser notificado él mismo y lograr prioridad para realizarse un test, o no asistir al trabajo o al lugar de estudio.

II-E. Geolocalización de infectados

En un esquema RDP descentralizado (como DP-3T o el propuesto por Google y Apple), es posible geolocalizar usuarios infectados a partir de la información intercambiada por bluetooth en el sistema. Una manera, presentada en [8], es que los usuarios, además de los identificadores, registren la ubicación donde se dio el contacto (por ejemplo con el uso de una aplicación diseñada a tales propósitos). Si muchos usuarios registran esta información y la comparten (algo similar a lo que sucede con la ubicación de cámaras o puestos de control de tránsito, por ejemplo) se puede lograr ver con cierta claridad los movimientos de las personas que (a posteriori) resulten infectadas.

El mismo efecto se logra mediante la colocación masiva de receptores bluetooth en una ciudad. Este último caso es estudiado y modelado en [9]. El resultado de una simulación de un ataque de este estilo se puede ver en la figura 1. Esta información puede ayudar además a identificar a las personas infectadas, deduciendo su identidad a partir de sus posibles movimientos por la ciudad[1].

[1]La posibilidad de asociar localizaciones con usuarios (anonimizados), como se muestra con trazos de diferentes colores en la figura 1, depende de cómo se implemente concretamente un sistema RDP descentralizado. Esta asociación de hecho es sencilla en las implementaciones de DP-3T (diseño 1) o el propuesto por Google y Apple.

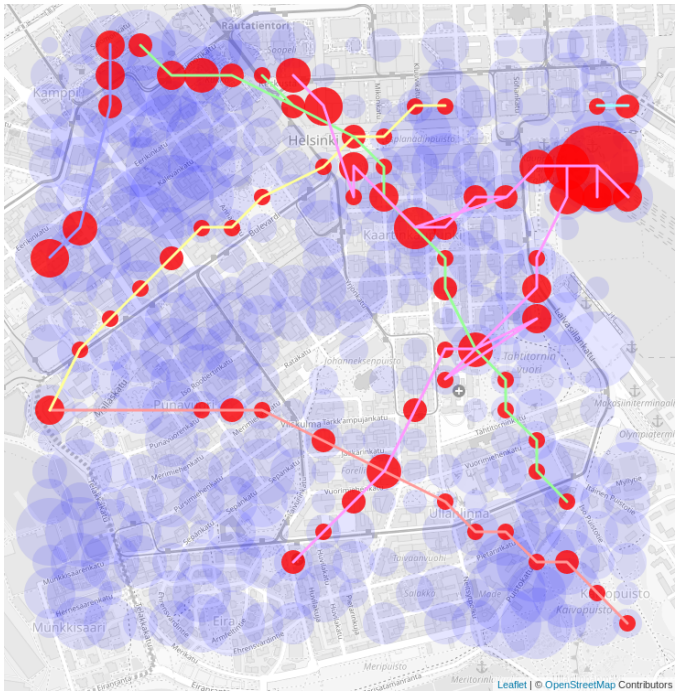

Figura 1. Resultado de simulación en [9], mostrando el movimiento de usuarios infectados en un esquema descentralizado

Cabe mencionar que, en esquemas descentralizados, la realización de este tipo de ataques solo requiere un tiempo de contacto pequeño, suficiente como para registrar la emisión de algún identificador, pero en general menor que el tiempo a partir del cual se estima una probabilidad alta de contagio. Para que un ataque de estas características sea efectivo en un esquema centralizado debe ser realizado por personas con acceso al servidor central (ya sea porque son los administradores, porque tienen la autoridad para hacer colaborar a los administradores, o porque logran infiltrarse en el sistema). En este caso se puede saber con certeza cuáles de los identificadores (y sus ubicaciones asociadas) corresponden a una misma persona, aunque en principio no se sabe quién es.

II-F. Revelamiento de interacciones sociales

Todos los sistemas de RDP analizados almacenan en el dispositivo de un usuario los identificadores recibidos de parte de otros participantes, junto con información temporal del momento en que fueron recibidos. Estos datos, por sí solos, revelan información privada potencialmente sensible. Por ejemplo, el hecho de que en determinado momento se haya recibido una gran cantidad de identificadores de parte de otros dispositivos puede usarse para inferir que el usuario participó en un evento con alta concurrencia de gente, como , por ejemplo, una manifestación, un espectáculo o un evento social.

Si un atacante tiene acceso a los registros de cierto dispositivo puede intentar inferir contactos sociales más específicos. Por ejemplo, si conoce algunos de los identificadores emitidos por el dispositivo de un tercero, puede determinar si se encontraron en algún momento. También podría realizar por sí mismo un cálculo de riesgo de contagio a partir de la

información contenida en el dispositivo, diferente (por ejemplo más sensible) que el calculado por el sistema de RDP, lo cual podría llevar a situaciones de discriminación.

II-G. Riesgos por el uso de Bluetooth

El hecho de que el funcionamiento de un sistema de RDP dependa de la tecnología Bluetooth establece de por sí riesgos, algunos de las cuales ya han sido descritos en las secciones anteriores. Adicionalmente, un atacante puede impedir el funcionamiento del sistema en un área determinada utilizando un bloqueador de señales de Bluetooth (Bloototh jammer).

Además, el sólo hecho de requerir el uso de la tecnología Bluetooth puede presentar un riesgo de seguridad para los usuarios: la tecnología puede presentar vulnerabilidades que pueden ser explotadas para realizar ataques informáticos sobre los dispositivos o vulnerar la privacidad de los usuarios (por ejemplo identificarlos y rastrearlos [10]). Es por esto que no se recomienda mantener encendida constantemente la funcionalidad de Bluetooth de los dispositivos como requeriría una solución de RDP.

Por otra parte es posible rastrear dispositivos bluetooth utilizando su dirección física, razón por la cual la mayoría de los dispositivos modernos utilizan direcciones ficticias que cambian cada pocos minutos. En el contexto de una solución de RDP, que a su vez emite identificadores temporales, es necesario que el cambio de dirección física y el cambio de identificador se haga de manera sincronizada. De otro modo, es posible para un atacante hacer el rastreo del dispositivo a medida que cambia uno de los dos datos. Como la gestión de direcciones físicas se hace a nivel del sistema operativo, sólo es posible resolver adecuadamente este problema si el sistema operativo del dispositivo brinda soporte para esto. Por ejemplo en dispositivos celulares, sólo soluciones que hagan uso de la tecnología de Google y Apple podrán resolver adecuadamente este problema.

Finalmente, como la información emitida a través de Bluetooth por los sistemas RDP es visible para cualquier observador, esto revela si alguien está usando la aplicación de rastreo o no. Por lo tanto, el solo hecho de poner en funcionamiento un sistema RDP pone en riesgo la privacidad de la decisión individual de participar o no del sistema.

III. Descripción de soluciones de RDP

En los primeros meses del año 2020 han surgido distintas iniciativas en relación al diseño, implementación y despliegue de tecnologías de RDP. En [11] se presentan y discuten las distintas alternativas de soluciones que han sido propuestas para implementar sistemas de este tipo. Algunas de ellas han sido ya desplegadas y están siendo actualmente usadas por residentes de los países donde se han implantado.

La mayoría de las propuestas se basan en la tecnología Bluetooth, más precisamente *Bluetooth Low Energy (BLE)*, transmitiendo y almacenando identificadores en el dispositivo móvil. Todas las que cuentan con implementaciones incluyen aplicaciones móviles para los sistemas operativos IOS y Android. En el caso de la iniciativa Apple & Google se trata de una API (Application Programming Inteface) para utilizar en desarrollos de aplicaciones específicas.

En general, estas soluciones siguen a grandes rasgos alguna de las dos alternativas de diseño predominantes: descentralizada o centralizada, las cuales se describen la sección III-A. A los efectos de fijar ideas y elaborar una discusión sobre bases concretas, en las secciones III-B y III-C se detalla un ejemplo de diseño descentralizado (DP-3T) y centralizado (ROBERT), respectivamente.

III-A. Alternativas de diseño

Con el objetivo de definir un marco de referencia de discusión de la problemática de seguridad y privacidad en sistemas RDP, en este trabajo hemos decidido estructurar el análisis en torno a lo que podríamos decir son los dos enfoques que se han tornado referentes:

1. El enfoque llamado *descentralizado*, en el que el cómputo de la verificación de exposición se realiza en el dispositivo móvil, y que denominaremos Escenario 1. Ejemplos de este tipo de diseños se encuentran en [12, 13, 2, 5].
2. El enfoque llamado *centralizado*, en el que el cómputo de la verificación de exposición se realiza en el servidor central, y que denominaremos Escenario 2. Este es el caso de los esquemas presentados en [14, 3].

La figura 2 presenta un diagrama operativo que describe la esencia del enfoque descentralizado, mientras que la figura 3 lo hace de un enfoque centralizado.

En ambas figuras se ilustra esquemáticamente las acciones que desarrolla cada actor y las interacciones que se dan entre ellos, a lo largo del funcionamiento de un sistema RDP. Los actores que participan son dos usuarios de ejemplo, sus dispositivos móviles, un servidor central y la autoridad de salud. En el ejemplo que se ilustra en las figuras, ambos usuarios se encuentran en determinado momento, tiempo después el usuario 1 es diagnosticado con COVID-19, y el usuario 2 se entera luego de que ha estado en riesgo. Las acciones e interacciones presentadas en las figuras están agrupadas en cuatro etapas:

1. *Preparación*: comprende los pasos necesarios para que un usuario comience a participar en el sistema RDP.
2. *Operación normal*: refiere a las operaciones que tienen lugar mientras ambos usuarios están sanos.
3. *Paciente positivo*: Detalla las acciones que se desencadenan cuando el usuario 1 es diagnosticado positivo.
4. *Verificación de exposición*: Describe los pasos que llevan a que el usuario 2 se entere de que ha estado expuesto a riesgo de contagio.

La operativa normal (etapa 2) es esencialmente la misma en ambos esquemas: los dispositivos móviles de los usuarios emiten y reciben continuamente Ids anonimizados y almacenan tanto los Ids recibidos como los emitidos. Los Ids que emite cada usuario son generados durante la etapa 1 de forma muy diferente según el escenario en cuestión. En el escenario descentralizado estos Ids son generados por el propio dispositivo de cada usuario, mientras que en un escenario centralizado es el servidor central el que se encarga de generarlos y enviarlos al dispositivo de cada uno. En las etapas 3 y 4 también se

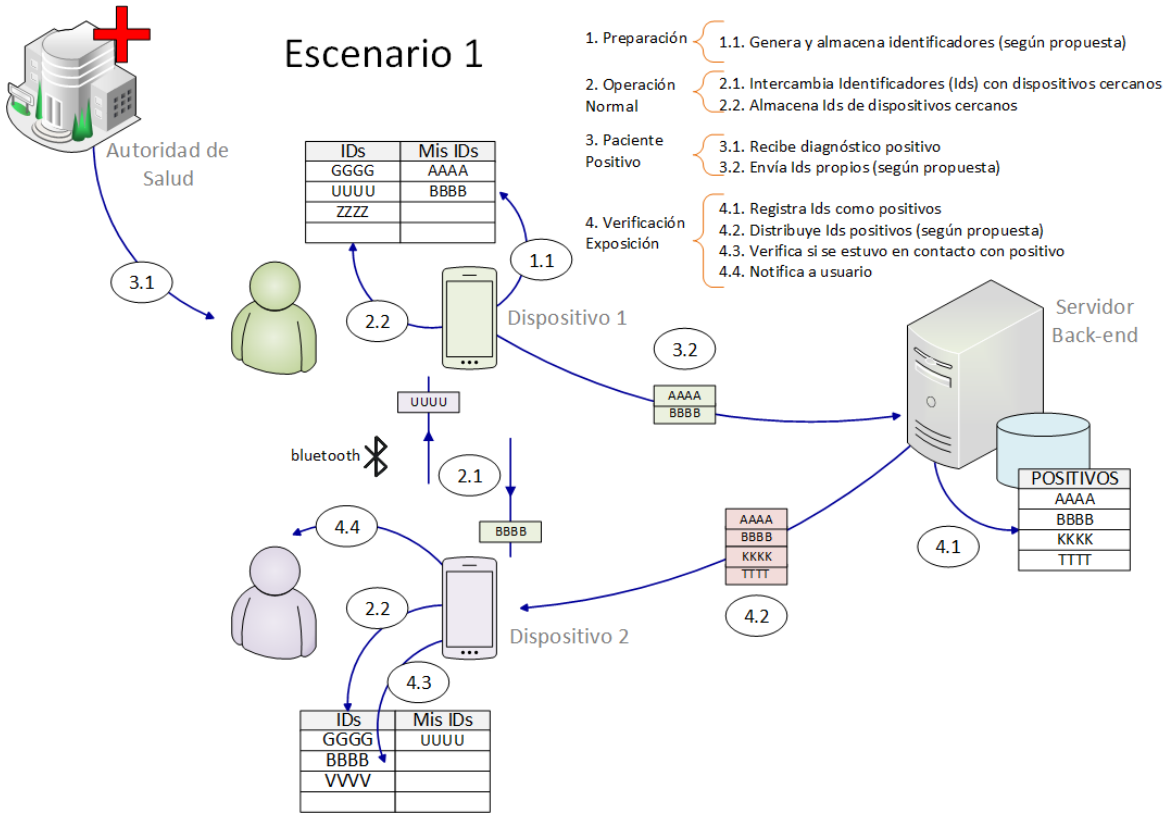

Figura 2. Solución descentralizada

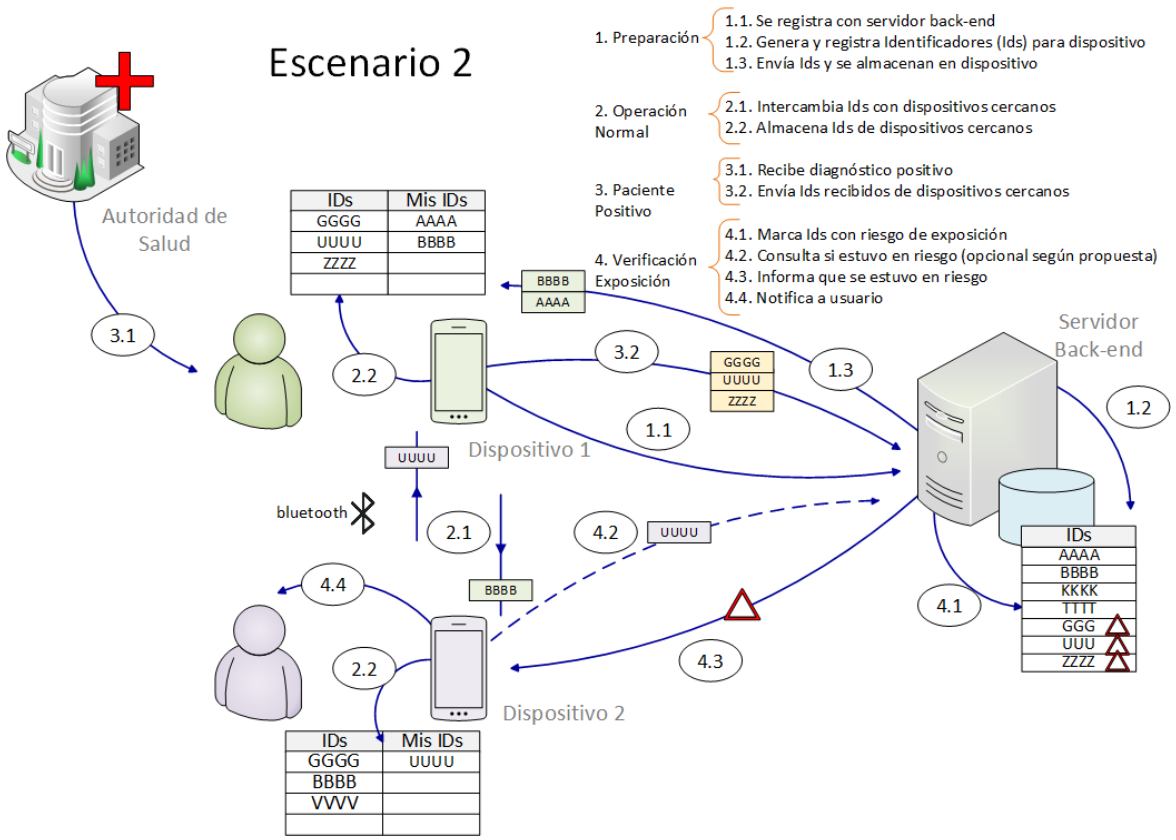

Figura 3. Solución centralizada

observan diferencias notorias. Mientras que en un escenario descentralizado el usuario 1 comunica al servidor central sus propios Ids generados y emitidos por su dispositivo (AAAA y BBBB en la figura 1), en el escenario centralizado envía los Ids que recibió de parte de otros usuarios (GGGG, UUUU, ZZZZ en la figura 2). En este último caso, al recibir el Id UUUU, el servidor central detecta que el usuario 2 (anonimizado) ha estado expuesto (recordar que fue el servidor central quien generó este Id para el usuario 2) y puede notificarle dicho riesgo a través de su dispositivo móvil. Por otra parte, en el escenario descentralizado el servidor central no es capaz de detectar por sí mismo que el usuario 2 ha estado expuesto a partir de los Ids AAAA, BBBB, emitidos por el usuario 1. En cambio, el servidor central reenvía estos Ids al resto de los dispositivos participantes, para que ellos mismos evalúen el riesgo. En el ejemplo de la figura 1, el dispositivo del usuario 2 recibe el Id BBBB, detecta que lo ha recibido de parte del dispositivo de algún otro usuario (en este ejemplo del usuario 1), y notifica al usuario 2 de la situación.

El consorcio DP-3T [2] (Decentralized Privacy-Preserving Proximity Tracing) ha propuesto un esquema de solución para implementar rastreo de proximidad descentralizado. Por otro lado, el instituto de investigación INRIA y Fraunhofer AISEC propusieron el esquema ROBERT (ROBust and privacy-presERving proximity Tracing), que es un claro exponente de un sistema centralizado.

III-B. Ejemplo de esquema descentralizado: DP-3T

La propuesta de DP-3T incluye dos diseños alternativos, con diferentes relaciones de compromiso entre privacidad y requerimientos de cómputo y comunicación. A modo de ejemplo se presenta a continuación el diseño 1, que es el más económico desde el punto de vista de recursos necesarios; este diseño es muy similar al implementado por Google y Apple.

La etapa de preparación (etapa 1) en DP-3T consiste en la selección aleatoria, por parte de cada dispositivo móvil que comience a operar en el sistema, de una clave secreta a través de la cual se derivan los Ids que serán emitidos en el futuro desde ese dispositivo. Concretamente, si un dispositivo comienza a operar en cierto día t, se sortea una clave secreta, denotada SK_t, a partir de la cual se calcula un conjunto de Ids a ser emitidos, en orden aleatorio, durante el día t. Este cálculo se realiza aplicando funciones criptográficas a la clave SK_t. La clave SK_t para el día inicial t determina además las claves SK_i que serán utilizadas en los días subsiguientes, aplicando recursivamente una función criptográfica H,

$$SK_i = H(SK_{i-1}), \quad i > t\,.$$

Como la clave SK_t determina todos los Ids emitidos cada día por el dispositivo de un usuario, en caso de que este sea diagnosticado positivo (etapa 3), es suficiente desvelar al resto de los usuario el valor de SK_t, junto al día inicial del período de contagio, para que todos puedan verificar si han estado expuestos. Para ello, durante la operación normal (etapa 2), los dispositivos participantes almacenan localmente todos los Ids recibidos de parte de otros dispositivos, junto con el día en que fueron recibidos y datos adicionales útiles para evaluar el riesgo de exposición, como por ejemplo una estimación de la distancia al emisor. La verificación de exposición (etapa 4) consiste en recibir de parte del servidor las claves SK_t y el día inicial del período de contagio reportados voluntariamente por los usuarios diagnosticados positivos; a partir de esta información se recalculan los Ids emitidos por los dispositivos de estos usuarios cada día, y se compara estos Ids con los almacenados localmente.

III-C. Ejemplo de esquema centralizado: ROBERT

En el caso de ROBERT, que es un esquema centralizado, el servidor central juega un rol mucho más activo que en el ejemplo anterior. En este caso, previo a la puesta en funcionamiento del sistema, se instala en el servidor una clave secreta, K_S, que se usará para generar Ids para que sean emitidos por los dispositivos participantes. También se configuran en el servidor una clave federada, K_G, y un código de país, CC_S, con fines de ineroperabilidad internacional.

En la etapa 1, cuando un usuario se integra al sistema a través de su dispositivo, se define una clave simétrica entre el dispositivo y el servidor, K_A, que es utilizada para futuras comunicaciones privadas entre ambos. También se establece una sincronización temporal aproximada entre ellos, de modo que entre todos los dispositivos participantes, así como el servidor central, queda definida una partición del tiempo en intervalos de duración constante común a todos los participantes (a menos de un pequeño desfasaje de no más de un segundo). Estos intervalos se denominan *épocas*, y se enumeran a partir de un cierto instante inicial. Adicionalmente el servidor le asigna a cada dispositivo registrado un identificador único, ID_A, que no está vinculado a la identidad real del usuario, que debería permanecer anónimo. Aplicando una función criptográfica a este identificador, las claves privadas instaladas en el servidor, K_S y K_G, y el código de país, CC_S, el servidor genera y transmite al dispositivo un Id para cada una de las próximas T épocas.

Durante la operación normal del dispositivo de un usuario (etapa 2), este emite en cada época el Id que le fue asignado por el servidor para esa época, junto con un indicador de tiempo de mayor precisión que la duración de una época. A la concatenación del Id con el indicador de tiempo se la aplica una función criptográfica, usando la clave K_A compartida con el servidor, que se incluye como parte del mensaje emitido. El objetivo de este componente criptográfico en el mensaje emitido es prevenir la emisión de mensajes corruptos o que un Id legítimo pueda ser repetido en el futuro en otro contexto. Periódicamente el dispositivo se comunica con el servidor para obtener nuevos Ids. Durante la operación normal, los dispositivos verifican la validez temporal de los mensajes que reciben de parte de otros dispositivos participantes, y almacenan localmente los Id válidos, junto con el instante de tiempo en que fueron recibidos.

En la etapa 3, cuando un usuario es diagnosticado positivo, su dispositivo envía al servidor los pares de Id y tiempo de recepción de todos los mensajes que recibió durante el período de contagio. La comunicación al servidor de estos Ids y sus tiempos de recepción se realiza uno a uno, y mezclados junto

con los de otros usuarios también diagnosticados positivos, de forma que el servidor no pueda conocer con exactitud qué Ids fueron recibidos por un mismo usuario. Haciendo uso de su clave privada, K_S, el servidor obtiene el identificador ID_A asociado a cada uno de los Ids recibidos por dispositivos de usuarios diagnosticados positivos. Con esta información, el servidor evalúa el riesgo de que los respectivos emisores de esos Ids hayan sufrido un contagio y, si este riesgo supera cierto umbral, el ID_A correspondiente es marcado como *expuesto* en una base de datos del servidor.

La verificación de exposición por parte de otros usuarios (etapa 4) se reduce a una consulta privada (usando la clave compartida K_A) del dispositivo del usuario al servidor. Si el servidor detecta que el ID_A correspondiente está marcado como expuesto, la situación es comunicada al dispositivo, que a su vez notifica al usuario para que tome las medidas pertinentes.

IV. Riesgos identificados en escenarios específicos

En esta sección revisamos los riesgos resumidos en el cuadro I a la luz de cada uno de los escenarios presentados en la sección III-A. Para esto establecemos una correspondencia entre estos riesgos y las distintas etapas (y pasos específicos) definidos en los escenarios 1 y 2. Este mapeo identifica en qué aspecto específico del flujo de ejecución de cada escenario aplica cada riesgo identificado, agregando los riesgos particulares asociados a cada tipo de solución (descentralizada, centralizada).

En los cuadros II y III, se presenta el flujo específico de las soluciones DP-3T, mientras que en los cuadros IV y V se presenta el flujo específico para ROBERT. Estos flujos se corresponden con la descripción presentada para cada uno en las secciones III-B y III-C, respectivamente.

Estos cuadros muestran, en primer lugar, que muchos de los riesgos identificados son compartidos por ambos esquemas, como ya fue ilustrado en la sección II. Por ejemplo durante la operación normal del protocolo, ambos esquemas están expuestos en mayor o menor medida a RI1, RI2 y RG1 al RG6 (es decir, en ambos es posible identificar, rastrear y geolocalizar usuarios, prevenir notificaciones y causar falsas alarmas, entre otros). Los riesgos específicos asociados a cualquier sistema que registra Ids recibidos por BLE son compartidos también por ambos esquemas: RE1, RE2 considerando los datos que se guardan en el dispositivo móvil. Lo mismo sucede en cuanto a los riesgos asociados a sistemas conectados en red RR1 y RR2 al momento de siendo positivo, subir los Ids registrados al servidor.

En donde ambos enfoques difieren es en la dificultad para llevar adelante estos ataques por parte de los distintos tipos de usuarios. Por ejemplo, para que un usuario logre identificar una persona infectada en el caso descentralizado alcanza con relacionar los identificadores recibidos por bluetooth con la persona (por ejemplo llevando un registro de las personas con las que estuvo en contacto en cada momento), en el caso centralizado el ataque requiere que el usuario registre varios dispositivos en el sistema y los vaya utilizando de manera de poder inferir el momento y lugar de contacto una vez que recibe una notificación.

Estas diferencias son en parte consecuencia de enfoques distintos sobre la problemática de privacidad y en particular al modelo de atacante utilizado por ambos enfoques. En el modelo centralizado la prioridad está puesta en proteger al sistema de posibles abusos por parte de usuarios individuales, mientras que en el modelo descentralizado el foco está puesto en proteger al sistema de posibles abusos por parte de la autoridad central que controla el servidor central o de actores maliciosos que logren acceso no autorizado al mismo.

Adicionalmente, existen riesgos específicos asociados al tipo de esquema que deben ser considerados. Por ejemplo, en el caso de sistemas centralizados, donde el servidor central juega un papel de mayor importancia, los Ids permanentes de los usuarios y de los contactos de los positivos son conocidos por el servidor. Esto determina que un *"servidor honesto pero curioso"* [15] a partir de los datos registrados pueda, por ejemplo, reconstruir el grafo (parcial) de interacción social en torno a usuarios positivos e identificar positivos (RP-CE3 y sub-riesgos asociados a SR5, SR6, SR8 y SR9 en [15]), así como habilitar el rastreo de ubicaciones en el tiempo y etiquetado de usuarios (RP-CE1 y sub-riesgos asociados a SR7 [15]). En este esquema existe también el riesgo de brechas y fuga de datos del servidor central, que permitiría hacerse con los Ids permanentes de los usuarios (RS-CE1), por lo que cobra aún más importancia la seguridad de la información en este servidor.

V. Consideraciones finales

En los primeros meses del año 2020 han surgido distintas iniciativas en relación al diseño, implementación y despliegue de tecnologías de rastreo digital de proximidad. En general, estas soluciones siguen a grandes rasgos alguna de las dos alternativas de diseño predominantes: descentralizada o centralizada. En este artículo se han identificado precisamente los flujos de datos y procesos involucrados en el funcionamiento de estas dos alternativas, así como los de dos propuestas concretas de cada una como son DP3T y ROBERT.

Aunque hayan sido diseñadas con foco en la protección de la privacidad de los usuarios, por las características de funcionamiento, todas las propuestas de RDP sufren de problemas intrínsecos de seguridad y privacidad que fueron descritas en este artículo. Por otra parte, hasta donde se sabe, la efectividad de estas aplicaciones aún es muy incierta, mientras que los riesgos reportados en la literatura especializada en los últimos meses son verosímiles y en muchos casos no requieren ninguna habilidad informática particular.

Este trabajo intenta contribuir al debate público brindando elementos técnicos y jurídicos a las autoridades y a la población en general para una toma de decisiones más informada de los riesgos reales y de lo que una aplicación de RDP podría, o no, garantizar en cuanto a la privacidad de sus usuarios.

En este sentido consideramos crucial identificar adecuadamente los procesos y utilizar los términos con el rigor científico que la situación exige (no es lo mismo seudonimizar datos que disociarlos o anonimizarlos). Por un lado, esto es

importante para valorar si realmente las tecnologías estudiadas cumplen con nuestro marco jurídico de protección de la salud, privacidad y libertad de nuestros habitantes, extremo que hasta el momento no es posible afirmar de modo alguno. Por otro lado, es necesario para cumplir cabalmente con el deber de informar a la población al momento de requerir su consentimiento, explicándole lisa y llanamente hasta dónde llega el (escaso) control que desde nuestro país podría existir sobre sus datos si decide utilizar las tecnologías de rastreo (artículo 12 de la Ley Nº 18.331, de 11 de agosto de 2008). Una errónea o defectuosa información vicia de nulidad el consentimiento.

Esperamos que este sea un insumo de valor al desarrollar y desplegar una solución de rastreo de proximidad y analizar si los posibles beneficios que brindaría su uso amerita tomar estos riegos.

Resaltamos además, que una implementación particular de estas tecnologías debe enfrentar desafíos de seguridad específicos y adicionales a los planteados en este artículo. El plan de este equipo de investigación es continuar trabajando en esta línea para generar recomendaciones de seguridad para una eventual implantación de RDP a nivel nacional.

Referencias

[1] G. Betarte, J. D. Campo, A. Delgado, P. Ezzatti, A. Forteza, L. González, A. Martín, B. Muracciole, and R. Ruggia, "Métodos y técnicas para soporte automatizado de la gestión de brotes de enfermedades infecciosas," April 2020. [Online]. Disponible: https://www.fing.edu.uy/inco/proyectos/protect

[2] C. Troncoso *et al.*, "Decentralized Privacy-Preserving Proximity Tracing," Tech. Rep., 2020. [Online]. Disponible: https://github.com/DP-3T/documents (Accedido: 3 de junio de 2020).

[3] "ROBERT: ROBust and privacy-presERving proximity Tracing," PRIVATICS team, Inria, France and Fraunhofer AISEC, Germany, Tech. Rep., 2020. [Online]. Disponible: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf (Accedido: 3 de junio de 2020).

[4] The StopCovid Project, "The StopCovid project," Tech. Rep., 2020. [Online]. Disponible: https://www.inria.fr/en/le_projet_stopcovid (Accedido: 3 de junio de 2020).

[5] G. Inc., "Apple and Google partner on COVID-19 contact tracing technology," April 2020. [Online]. Disponible: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (Accedido: 3 de junio de 2020).

[6] The DP-3T Project, "Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems," Tech. Rep., 2020. [Online]. Disponible: https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf (Accedido: 3 de junio de 2020).

[7] Fraunhofer AISEC, "Pandemic Contact Tracing Apps: DP-3T, PEPP-PT NTK, and ROBERT from a privacy perspective," Tech. Rep., 2020. [Online]. Disponible: https://eprint.iacr.org/2020/489 (Accedido: 3 de junio de 2020).

[8] X. Bonnetain *et al.*, "Anonymous tracing, a dangerous oxymoron: A risk analysis for non-specialists," Tech. Rep., 2020. [Online]. Disponible: https://tracing-risks.com/ (Accedido: 3 de junio de 2020).

[9] Otto Seiskari, "BLE contact tracing sniffer PoC." [Online]. Disponible: https://github.com/oseiskar/corona-sniffer (Accedido: 3 de junio de 2020).

[10] G. Celosia and M. Cunche, "Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile," in *IoT S&P 2019 - 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*. London, United Kingdom: ACM Press, Nov. 2019, pp. 24–31. [Online]. Disponible: https://hal.inria.fr/hal-02359914

[11] G. Betarte, J. D. Campo, A. Delgado, P. Ezzatti, A. Forteza, L. González, A. Martín, B. Muracciole, and R. Ruggia, "Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo de proximidad," Proyecto *PROTECT*, Tech. Rep., May 2020. [Online]. Disponible: https://www.fing.edu.uy/inco/proyectos/protect/docs/protect_position_050520.pdf

[12] R. Raskar, "Private kit: Safe paths - can we slow the spread without giving up individual privacy?" March 2020. [Online]. Disponible: https://safepaths.mit.edu/ (Accedido: 3 de junio de 2020).

[13] Covid Watch, March 2020. [Online]. Disponible: https://covid-watch.org (Accedido: 3 de junio de 2020).

[14] J. Bay *et al.*, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders," Government Technology Agency - Singapore, Tech. Rep., 2020. [Online]. Disponible: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf (Accedido: 3 de junio de 2020).

[15] The DP-3T Project, "Security and privacy analysis of the document "ROBERT: ROBust and privacy-presERving proximity Tracing," Tech. Rep., 2020. [Online]. Disponible: https://github.com/DP-3T/documents/blob/master/Security%20analysis/ROBERT%20-%20Security%20and%20privacy%20analysis.pdf (Accedido: 3 de junio de 2020).

Cuadro II
ANÁLISIS DP-3T (EJEMPLO ESCENARIO DESCENTRALIZADO) - PARTE 1

Dispositivo Móvil	Servidor Back-end	Riesgos Privacidad (RP)	Riesgos Seguridad (RS)
1.PREPARACIÓN			
1.1 – Genera clave aleatoria SK_t para el día actual t. La clave SK_t determina un conjunto de Ids a ser emitidos durante cada día de aquí en más. Cada día el dispositivo sortea un orden aleatorio para la emisión de los Ids de ese día.			
2.OPERACIÓN NORMAL			
2.1 – Intercambia por BLE los **Ids generados** con otros dispositivos en proximidad física cercana.		**RI 1, RG 3, RG 5, RG 6** **(RP-DE1) Obtener ubicaciones:** Si se tiene acceso a los Ids emitidos que se almacenan en un dispositivo, se podría determinar si la víctima ha estado en determinados lugares monitoreados por el atacante. Parcialmente mitigado por rotación de Ids y uso de herramientas criptográficas ([6, pp 13]).	**RI 2, RG 1, RG 2, RG 4** **(RS-DE1) Riesgo de datos comprometidos en el dispositivo**: se requiere constante transmisión y registro de Ids, con sistema ejecutando en background. En dispositivos Apple esto no es posible si no se implementa a través de la API definida con Google; si no se usa esta API se requieren workarounds ej. ejecución fuera de background con pantalla y dispositivo no bloqueado y sin protección de contraseña. En el caso de robo o pedido de la policía, todos los datos quedan expuestos [15, pp 10-11]
2.2 - Registra los Ids recibidos de dispositivos cercanos junto con el día en que fueron recibidos e información adicional útil para evaluar el riesgo de contagio.		**RE 1, RE 2**	

Cuadro III
ANÁLISIS DP-3T (EJEMPLO ESCENARIO DESCENTRALIZADO) - PARTE 2

Dispositivo Móvil	Servidor Back-end	Riesgos Privacidad (RP)	Riesgos Seguridad (RS)
3.PACIENTE POSITIVO			
3.1 - Diagnosticado como positivo aprueba enviar sus Ids.			
3.2 - Envía su clave SK_t y el día inicial del período de contagio.		**RR1, RR 2**	**RI 3**
4.VERIFICACIÓN EXPOSICIÓN			
	4.1 – Accede a las claves y días iniciales del período de contagio comunicados voluntariamente por los usuarios con diagnóstico positivo.		
	4.2 – Distribuye las claves y días iniciales del período de contagio al resto de los usuarios.		
4.3 – A partir de las claves y días iniciales del período de contagio de cada usuarios con diagnóstico positivo, recalcula los Ids emitidos por estos usuarios y evalúa, comparando con información almacenada localmente, el riesgo de contagio.			
4.4 – Notifica a usuario.			

Cuadro IV
ANÁLISIS ROBERT (EJEMPLO ESCENARIO CENTRALIZADO) - PARTE 1

Dispositivo Móvil	Servidor Back-end	Riesgos Privacidad (RP)	Riesgos Seguridad (RS)
1.PREPARACIÓN			
	1.0 – Instala clave secreta K_S, clave federada K_G, y código país.		
1.1 – Se registra con servidor. Esto requiere una demostración de trabajo (ej. CAPTCHA) para evitar registros automáticos o ataques de negación de servicio. Establece clave simétrica K_A compartida con el servidor y sincroniza épocas con el servidor. Obtiene Ids para las próximas T épocas (este paso se repite periódicamente).			
	1.2 – Genera identificador único (ID_A) para el dispositivo. - Establece clave simétrica K_A compartida con el dispositivo. - Genera Ids para que el dispositivo emita durante las próximas T épocas.	**(RP-CE1) Function creep** – convertir en instrumento de vigilancia más allá del COVID-19, vinculando los Ids de cualquier usuario, el servidor puede: **(RP-CE1.1)** Habilitar el rastreo de individuos en el tiempo, combinando con otras bases de datos para obtener identidad real del usuario [15, pp 2-3]. **(RP-CE1.2)** Etiquetar y clasificar individuos que puedan ser reconocidos luego por terceras partes sin necesitar del servidor (ej. Policía) [6, pp 19 SR7].	**(RS-CE1)** Clave comprometida – no se especifica rotación de claves, si se logran obtener las claves del servidor: -clave secreta K_S, es posible conocer los identificadores únicos, ID_A, de todos los usuarios a partir de los Ids que emite. - clave federada K_G, se conocen todos los códigos de los países [15, pp 10].
	1.3 - Envía periódicamente Ids a emitir a los dispositivos registrados.		
2.OPERACIÓN NORMAL			
2.1 – Intercambia Ids recibidos por BLE con otros dispositivos en proximidad física cercana.		**RI 1, RG 3, RG 5, RG 6**	**RI 2, RG 1, RG 2, RG 4** **(RS-CE2) Riesgo de datos comprometidos en el dispositivo**: se requiere constante transmisión y registro de Ids, con sistema ejecutando en background. En Apple esto no es posible, y la nueva API solo permite consultar por Ids para verificar exposición, en particular **no provee funcionalidad para enviar lista de Ids**. Se requieren workarounds ej. ejecución fuera del background con pantalla y dispositivo no bloqueado y sin protección de contraseña. En el caso de robo o pedido de la policía, todos los datos quedan expuestos [15, pp 10-11].
2.2 - Registra los Ids recibidos de dispositivos cercanos junto con el instante de tiempo en que fueron recibidos.		**RE 1, RE 2**	

Cuadro V
ANÁLISIS ROBERT (EJEMPLO ESCENARIO CENTRALIZADO) - PARTE 2

Dispositivo Móvil	Servidor Back-end	Riesgos Privacidad (RP)	Riesgos Seguridad (RS)
3.PACIENTE POSITIVO			
3.1 – Diagnosticado como positivo aprueba enviar sus datos, con autorización de salud.			
3.2 - Envía todos los Ids recibidos desde otros dispositivos durante el período de contagio, junto con el tiempo de recepción de cada uno. Los Ids registrados se transmiten en envíos independientes (de a uno), mezclados los Ids comunicados por otros usuarios.		**RR 1, RR 2** **(RP-CE2) Mecanismo de anonimización de canal**: Debe preverse un mecanismo para evitar que el conjunto de Ids subidos por un usuario sean fácilmente distinguibles de los Ids subidos por otro usuario (en [3, sección 6.1] se sugieren alternativas) [15, pp 9-10].	**RI 3** **(RS-CE3) Falsear riesgo**: al subir los Ids observados, el atacante podría inyectar Ids observados por otros usuarios o dispositivos, para que se marquen como expuestos al contagio otros individuos (por ejemplo, blancos específicos) ([15] pp 10) **VER también (RS-CE2)**
4.VERIFICACIÓN EXPOSICIÓN			
	4.1 – Accede a los Ids recibidos por los dispositivos de usuarios con diagnóstico positivo durante sus períodos de contagio. Obtiene el identificador único, ID_A, de los emisores de esos Ids (chequeando la validez de cada registro). Computa el riesgo de exposición y marca como expuesto.	**(RP-CE3) Ataques de enlace**: permiten obtener relaciones entre positivos que suben sus registros y sus contactos, identificar positivos, co-ubicación entre no infectados. Notar que en este esquema: el servidor conoce los identificadores ID_A de los usuarios asociados a cada uno de los Ids recibidos de parte de los positivos [6, SR9 pp 21]. Por esta razón este tipo de riesgos es particularmente sensible a la preservación de la pseudoanonimidad de usuarios (**ver RP-CE1.1**) **(RP-CE3.1) Enlace basado en timestamps**: ataques de intersección de timestamps podrían permitir estimar contactos entre infectados [15, pp 4-5], [6, SR5 pp 19]. **(RP-CE3.2) Co-ubicaciones basado en timestamps**: el enlace de infectados podría permitir además estimar co-ubicaciones entre infectados y no-infectados, construyendo una aproximación del grafo social de contactos [15, pp 5], [6, SR6 y SR8 pp 17 y 20]. **(RP-CE3.3) Identificar positivos anónimos con co-ubicaciones, causalidad y análisis de frecuencia**: análisis diversos de los datos subidos por positivos podrían permitir identificar positivos, contactos y aproximar grafo social [15, pp 5-9], [6, SR6 y SR8 pp 17 y 20].	
4.2 – Consulta periódicamente si estuvo en riesgo.			
	4.3 – Informa que estuvo expuesto y marca como notificado el ID_A asociado		
4.4 – Notifica a usuario.			