Análisis de la privacidad de WhatsApp Messenger

M. MÓJICA LÓPEZ, J. L. RODRIGO OLIVA, V. GAYOSO MARTÍNEZ, L. HERNÁNDEZ ENCINAS y A. MARTÍN MUÑOZ

Instituto de Tecnologías Físicas y de la Información (ITEFI), Consejo Superior de Investigaciones Científicas (CSIC)
Madrid, 28006, España

RESUMEN

El uso de aplicaciones de mensajería instantánea se ha vuelto cada vez más cotidiano para una gran parte de la población, donde la aplicación WhatsApp Messenger es una de las más populares a nivel mundial. Los datos asociados a cada cuenta de usuario de WhatsApp, como las fotos de perfil, los estados o el número de teléfono, son información personal que es visible para cualquier tercero con la configuración por defecto establecida tras la instalación.

En este trabajo se ha desarrollado una aplicación para Android que escanea un rango de números de teléfono y obtiene, para cada número que tenga cuenta de WhatsApp, los cambios de los estados y las imágenes de perfil que el usuario haya introducido. El objetivo de esta contribución es evaluar el nivel de privacidad que WhatsApp Messenger presenta con este modelo de configuración por defecto, analizando para ello un grupo de usuarios de gran tamaño.

Palabras clave: Android, Mensajería instantánea, Privacidad, Smartphones, WhatsApp

1. INTRODUCCIÓN

El uso de los servicios de mensajería instantánea, conocidos comúnmente por su denominación en inglés Instant Messaging (IM), ha crecido enormemente en la última década, especialmente en lo que se refiere a las aplicaciones móviles que proveen este tipo de servicio. El acceso cada vez más extendido a los *smartphones* por parte de la población mundial ha jugado un papel muy importante en el desarrollo y evolución de estas aplicaciones.

Desde que salió al mercado la primera generación de iPhone en 2007 [1] y el primer móvil con sistema operativo Android, lanzado a finales de 2008 [2], han surgido multitud de aplicaciones de mensajería instantánea. Disponer de un *smartphone* se ha convertido en algo muy común en muchas partes del planeta: según un estudio del Pew Research Center, el 43 % de la población mundial tenía un *smartphone* en 2016 [3]. Con el tiempo, la mensajería instantánea ha ido sustituyendo paulatinamente a los SMS (Short Message Service), debido a la ventaja que supone el funcionamiento de estas aplicaciones a través de la red de datos móviles o una conexión Wi-Fi [4].

A causa del uso tan extendido que se hace de estas aplicaciones, especialmente en al ámbito personal, se demandan mejoras en la implementación de los servicios en términos de seguridad y privacidad. De esta manera, los desarrolladores de estas aplicaciones se preocupan cada vez más por implementar mejores tecnologías de cifrado para el envío de los mensajes, añaden más opciones de seguridad y privacidad y se preocupan por ofrecer una política de privacidad más garantista con los usuarios. Además, será necesario entender las implicaciones que tiene el comportamiento de los usuarios de cara a garantizar la seguridad y privacidad [5].

El presente trabajo tiene como objetivo realizar un análisis de la privacidad del servicio de mensajería instantánea que ofrece WhatsApp Inc. Para ello, como herramienta principal de extracción de datos se ha desarrollado una aplicación para Android que escanea un rango de números de teléfono y asocia a cada número que tenga cuenta de WhatsApp Messenger (en adelante WhatsApp) un registro con los cambios de los estados y las imágenes de perfil o avatar del usuario. Esta aplicación ha sido diseñada con el objetivo de ser ejecutada en una maquina virtual, por comodidad en el desarrollo de las pruebas, aunque también podría ser ejecutada en un dispositivo móvil.

El motivo de la extracción de estos datos se basa en que los mismos conforman información personal que permite identificar total o parcialmente al usuario, además de posibilitar la obtención de información sobre sus hábitos o costumbres.

Existen varios trabajos de investigación previos que incluyen un análisis de la privacidad de WhatsApp, como el realizado por Schrittwieser et al. en 2012 [6], el desarrollado por Martijn Terpstra en 2013 [7] o el realizado por N. Rastogi y J. Hendler en 2017 [8]. Los tres coinciden en resaltar la debilidad que supone la autenticación del usuario mediante el número de teléfono, identificando como una vulnerabilidad de privacidad el acceso a los datos personales de los usuarios precisamente mediante el número de teléfono. También mencionan como vulnerabilidad el escaneo de la lista de contactos por parte de WhatsApp y el acceso a otros metadatos como los sellos de tiempo (*timestamp*) de los cambios de estado o los tiempos de conexión. Adicionalmente, existe un estudio de 2015 realizado con la aplicación de mensajería KaKaoTalk, muy popular en Corea, con conclusiones similares [9].

A diferencia de las investigaciones anteriores, en este trabajo se incluye un análisis de las imágenes de avatar que los usuarios hacen visibles, siendo este el motivo principal de que la extracción de datos sea más lenta que en los otros estudios. Solo en las investigaciones [6] y [9] se ha realizado algún experimento de escaneo de contactos y análisis de los datos obtenidos. El trabajo [6] es el que más se asemeja a nuestra investigación; sin embargo, este se llevó a cabo en 2012, cuando WhatsApp solo contaba con aproximadamente 200 millones de usuarios, a diferencia de hoy que ya alcanza los 2.000 millones [10], por lo que los resultados han perdido validez. Aunque en [6] se menciona que se realizó un escaneo de 10 millones de contactos de un rango de teléfonos de la ciudad de San Diego, no se explicita que métodos se utilizaron para realizarlo. En cambio, en el presente trabajo se describen detalladamente los mecanismos utilizados para extraer los datos, con la motivación de que esta investigación pueda ser replicada o extendida en el futuro. Por su parte, en las investigaciones [7] y [8] solo se

mencionan las vulnerabilidades de acceso a datos personales y metadatos, y en esta última se sugiere una posible aplicación web de escaneo de contactos, pero no se realiza ninguna extracción de datos.

Con esta intención, en el presente artículo, la Sección 2 proporciona un acercamiento al campo de las aplicaciones móviles de mensajería instantánea y describe las características técnicas de WhatsApp más relevantes para este análisis. A continuación, la Sección 3 realiza una descripción detallada de la aplicación desarrollada para la extracción de datos, mientras que la Sección 4 muestra los resultados obtenidos en esta investigación. Finalmente, la sección 5 expone las conclusiones tras el análisis realizado.

2. APLICACIONES DE MENSAJERÍA INSTANTÁNEA

A día de hoy, existe una gran variedad de aplicaciones de mensajería instantánea para móviles. En términos generales, su funcionalidad principal consiste en el envío de mensajes de forma instantánea a otros usuarios de este servicio. Los mensajes son principalmente de texto, aunque muchas aplicaciones también permiten el envío de fotos, vídeos o notas de audio. Otras funcionalidades que se ofrecen son la creación de grupos o canales de difusión y las videollamadas. Todas estas aplicaciones, conocidas en este contexto como Over-the-top Applications (OTT) [11], funcionan sobre la red de datos móviles o a través de una conexión Wi-Fi.

Es muy común que una misma aplicación se desarrolle para los principales sistemas operativos de teléfonos móviles, destacando los desarrollos para Android y para iOS, aunque también existen aplicaciones para Windows Phone o Blackberry OS, buscando la mayor compatibilidad posible con los diferentes sistemas operativos presentes en el mercado.

La popularidad de las distintas aplicaciones varía según países y regiones del planeta. Por ejemplo, Line [12] es muy popular en Japón, imo [13] en Cuba, BBM [14] en Indonesia y WeChat [15] en China. Sin embargo, WhatsApp y Messenger de Facebook [16] son las más utilizadas a nivel global [17].

En febrero de 2016, WhatsApp anunció en su blog oficial que su número de usuarios ascendía a 2 mil millones de personas, pertenecientes a 180 países diferentes, lo cual implica que una de cada siete personas en el mundo utiliza este servicio de mensajería instantánea para comunicarse entre ellas [18]. La gran popularidad de WhatsApp ha sido el principal motivo para elegirla en este estudio.

En los últimos años han surgido aplicaciones menos conocidas, que se definen a sí mismas como "seguras" y afirman garantizar la privacidad y la seguridad de sus usuarios como característica destacada, incluyendo opciones de cifrado punto a punto, borrado de mensajes, elementos de identificación y verificación de las identidades de los usuarios, desarrollo en código abierto para poder hacer auditorías de seguridad, videollamadas cifradas [19], etc. Algunas de estas aplicaciones son Telegram [20], Signal [21], ChatSecure [22], Wikr [23] o Threema [24]. Siguiendo esta tendencia, algunas aplicaciones muy conocidas pero que no se definían por la protección de sus usuarios, han añadido recientemente funcionalidades relacionadas con la privacidad y la seguridad. En el caso de WhatsApp, se puede destacar el cifrado punto a punto que añadió en 2016 [25], junto con las funcionalidades de verificación de usuarios mediante códigos QR [26] o su renovada política de privacidad [27].

De esta manera, se pone de manifiesto que existe cierta preocupación por parte de los usuarios y las compañías por aumentar la privacidad y la seguridad en el uso de las aplicaciones de mensajería instantánea. Sin embargo, al mismo tiempo se pretende mantener unos altos niveles de usabilidad de las aplicaciones, lo que en muchas ocasiones se hace incompatible con el incremento de la seguridad y la privacidad. Por ejemplo, en la mayoría de las aplicaciones que se han citado, incluida WhatsApp, se utiliza el número de teléfono como identificador del usuario y, además, se debe permitir el escaneo de la agenda de contactos del usuario para poder iniciar la comunicación con otros usuarios, lo cual implica el acceso a información personal.

A continuación, se ofrece un breve resumen sobre la estructura de WhatsApp y su funcionamiento. Como ya se ha mencionado anteriormente, la aplicación genera su lista de contactos a partir de la agenda del teléfono y por eso, al instalarla, solicita permiso para acceder a ella. La agenda se escanea periódicamente y los contactos son guardados en una base de datos de la aplicación en formato SQLite denominada "wa.db" y cuyo contenido está descrito más adelante.

Los ficheros que la aplicación necesita están ubicados tanto en el almacenamiento interno como el externo del teléfono, cuyas principales características se comentan a continuación.

- Al almacenamiento externo del teléfono se tiene acceso total de lectura y escritura por parte de aplicaciones y usuarios. Aquí se almacenan todos los archivos multimedia que se envían y reciben (fotos, audios y videos) sin ningún tipo de cifrado. En cambio, las conversaciones sí se guardan en una base de datos cifrada pero, a pesar de ello, algunos investigadores han conseguido recuperar la clave de cifrado [28].

- El almacenamiento interno del teléfono es una zona de memoria más interesante ya que, a pesar de que solo es accesible desde terminales "rooteados" (un móvil "rooteado" es aquel cuyo sistema operativo ha sido modificado para tener control total sobre él), toda la información aquí almacenada carece de cifrado. En esta zona podemos encontrar las bases de datos que almacenan las conversaciones, las fotos de perfil de los contactos, sus estados, etc. [29]. En la Tabla 1 se muestra la estructura de los ficheros de este directorio.

WhatsApp tiene opciones de privacidad como por ejemplo el bloqueo de contactos y la confirmación de lectura de mensajes. Las que nos interesan en este artículo son las referentes al estado y a la foto de perfil, tal como se puede apreciar en la Figura 1. Por defecto, cuando WhatsApp se instala en el teléfono, cualquier otro usuario de la aplicación que agregue nuestro número a su agenda de contactos, podrá ver nuestro estado, foto de perfil y la última vez que nos conectamos.

3. APLICACIÓN DESARROLLADA

Tal como se ha mencionado anteriormente, en el contexto de esta investigación se ha desarrollado una aplicación para Android, pensada para ser ejecutada en una maquina virtual, y

	Contenido	Directorio	Fichero
1	Contactos	/data/data/com.whatsapp/databases	wa.db
2	Chats	/data/data/com.whatsapp/databases	msgstore.db
3	Avatares	/data/data/com.whatsapp/files/Avatars	<telefono>@s.whatsapp.net.j
4	Copia avatares	/data/data/com.whatsapp/cache/ProfilePictures	<telefono>@s.whatsapp.net.j
5	Registros	/data/data/com.whatsapp/files/Logs	whatsapp.log

Tabla 1. Estructura de ficheros de WhatsApp.

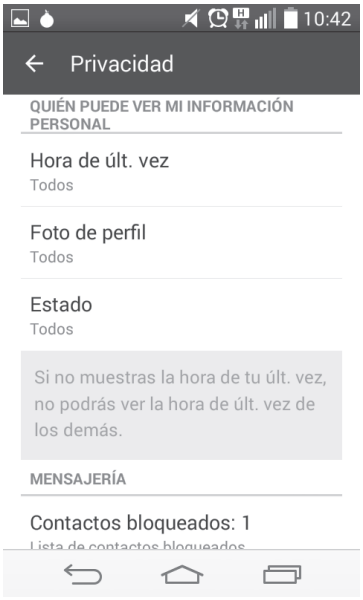

Figura 1. Opciones de privacidad de WhatsApp por defecto.

cuya principal utilidad consiste en extraer datos de los usuarios de WhatsApp en un rango de números de telefono determinado por el usuario. A esa aplicación se le ha dado el nombre de WhatsappScan y a partir de ahora nos referiremos a ella de esa manera. En la Figura 2 podemos apreciar el aspecto gráfico que presenta mientras que en la Tabla 2 podemos ver la estructura interna de sus ficheros.

La aplicación se divide en dos partes bien diferenciadas:

- El módulo encargado del escaneo de los usuarios de WhatsApp y la visualización de los datos. Esta es la parte que se encarga de actualizar la agenda de contactos, copiar las bases de datos de Whatsapp, rellenar las bases de datos propias de la aplicación y por último mostrar los resultados obtenidos.

- El módulo de grabación de movimientos. Esta parte es la que automatiza todo el proceso anteriormente comentado. Se trata de un sistema de grabación de clics y movimientos del ratón que permite reproducirlos más tarde automáticamente.

Escáner

WhatsApp guarda información de los contactos en una base de datos SQLite propia llamada "wa.db". Este fichero está situado en "/data/data/com.whatsapp/databases/" y tiene el formato indicado en la Tabla 3.

Con algunos elementos de esta base de datos, como el estado y la fecha en la que fue modificado, la aplicación forma otra base de datos con la estructura indicada en las Tablas 4, 5 y 6. Además, los ficheros que contienen las fotos de los contactos son guardados en la carpeta "files" de WhatsappScan.

Una vez lanzada la aplicación WhatsappScan, para iniciar el proceso de escaneo es necesario escribir el rango de números en los campos de texto "From" y "To". Posteriormente se pulsa el botón "Scan", lo que iniciará varias tareas. La primera de ellas se encarga de introducir el rango de contactos en la agenda del terminal para que WhatsApp los lea y los incorpore a su base de datos. Una vez terminada esta tarea, automáticamente se abre la aplicación WhatsApp. En este punto, la base de datos "wa.db" se ha actualizado con los contactos y sus estados. Sin embargo, para optimizar los recursos del sistema WhatsApp no actualiza las fotos al instante, sino que es necesario hacer un desplazamiento sobre la lista de contactos para que se realice dicha actualización.

Una vez que todos los contactos han sido actualizados podemos volver a WhatsappScan para pulsar el botón "View". En este momento es cuando se hace la copia de todos los datos de WhatsApp a las bases de datos de WhatsappScan. Se ha decidido hacer la copia en este punto y no antes puesto que hasta que no se visualiza por completo la lista de contactos, no se cargan las fotos y es imposible que el programa decida por sí solo en qué momento puede comenzar a extraer la información. Una vez que todos los datos han sido copiados, se muestra la

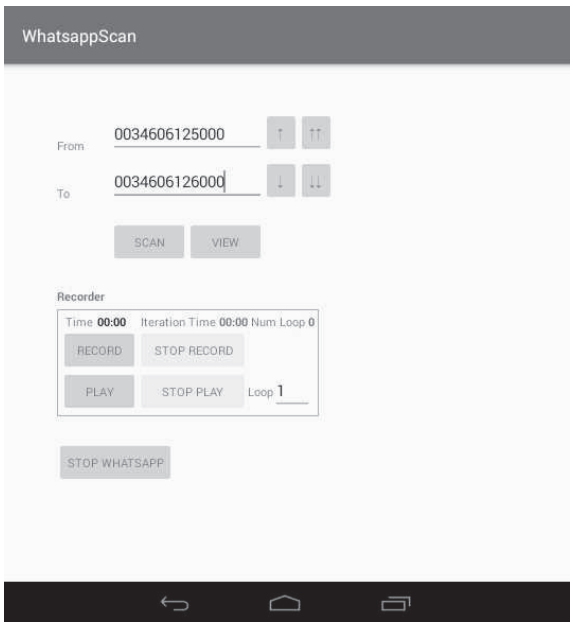

Figura 2. WhatsappScan.

	Contenido	Directorio	Fichero
1	Imágenes	/data/data/com.csic.whatsappscan/files/	<telefono>_<número_de_orden>.png
2	Fichero de la grabación	/data/data/com.csic.whatsappscan/cache/	eventsRecord.log
3	Base de datos de WhatsApp	/data/data/com.csic.whatsappscan/databases/	wa.db
4	Base de datos de WhatsappScan	/data/data/com.csic.whatsappscan/databases/	spy.db

Tabla 2. Estructura de ficheros del paquete WhatsappScan.

Campo	Descripcion
jid	Identificador del contacto
is_whatsapp_user	Contiene 1 si es usuario de whatsapp y 0 si no lo es
thumb_ts	Sello de tiempo indicando cuando fue modificado el avatar
status	Estado del contacto (es una cadena de texto)
status_timestamp	Sello de tiempo indicando cuándo fue modificado el estado

Tabla 3. Estructura de la tabla `wa_contacts` de wa.db.

Campo	Descripcion
id	Identificador del contacto
number	Número de teléfono

Tabla 4. Estructura de la tabla `spy_contacts`.

Campo	Descripcion
id	Identificador del contacto
number	Número de teléfono
photo_path	Nombre del fichero en la ruta /data/data/com.csic.whatsappscan/files/
thumb_ts	Sello de tiempo indicando cuándo fue modificado el avatar

Tabla 5. Estructura de la tabla `spy_photos`.

Campo	Descripcion
id	Identificador del contacto
number	Número de teléfono
status	Estado del contacto (es una cadena de texto)
status_timestamp	Sello de tiempo indicando cuándo fue modificado el estado

Tabla 6. Estructura de la tabla `spy_status`.

lista de contactos y sus historiales justo después de borrar la agenda del teléfono, a fin de optimizar los recursos.

Como se puede ver en las Figuras 3 y 4, los datos almacenados en las tablas antes descritas se presentan en forma de lista de contactos, mostrando el historial de cambios de fotos y estados junto con la fecha en la que los usuarios escaneados los realizaron.

Grabadora

Con la limitación antes mencionada a la hora de sincronizar la agenda de contactos con WhatsApp, si se pretende escanear cientos de miles de perfiles, es necesario hacerlo de una forma automática sin que se tenga que modificar manualmente el rango de teléfonos. Para esta tarea se ha programado el modulo "recorder". Gracias al comando de Linux "getevent" se puede capturar el movimiento del ratón, junto con sus clics, guardarlos en un fichero y posteriormente volver a lanzar ese movimiento con el comando "sendevent" tantas veces como sea necesario. Para ello, con los botones "Record" se graba una ejecución completa del programa, escaneando 1000 contactos. Posteriormente con el botón "Play" se puede reproducir esa ejecución tantas veces como ponga en el cuadro de texto "Loop", ejecutándose un número infinito de veces si se deja en blanco o se introduce un número negativo. En el caso de ejecutarse infinitamente, se puede cancelar pulsando el botón "Stop play".

Figura 3. Lista de contactos.

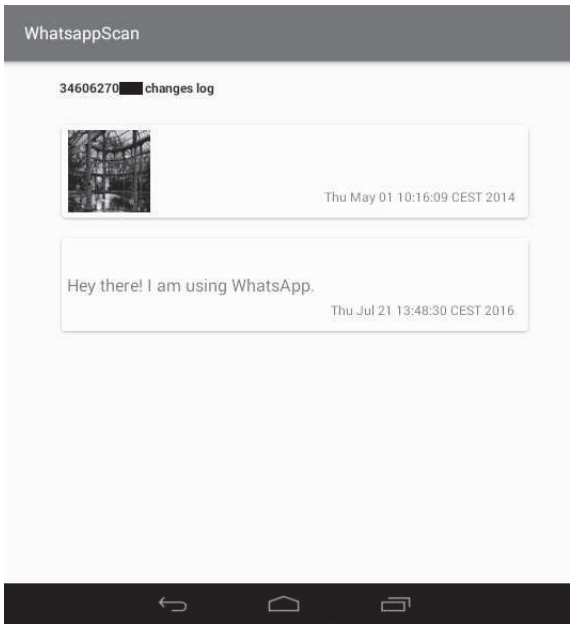

Figura 4. Historial de cambios.

Como se ha aclarado anteriormente, esta aplicación se ha ejecutado en una máquina virtual por cuestiones de comodidad en el desarrollo de las pruebas, aunque también puede ser ejecutada en un dispositivo móvil.

Para desarrollar esta funcionalidad se tomó como referencia el proyecto de GitHub "Adb Event Record" de T. Lin [30].

4. RESULTADOS

Contexto técnico

En las pruebas se ha utilizado una máquina virtual en Virtual Box, versión 5.0.20, con las siguientes características:

- Sistema operativo: Android 4.4.2 KitKat.
- Memoria RAM: 8 GB.
- Espacio en disco: 20 GB.
- Procesador: virtual de 4 CPU.
- Red: Adaptador Realtek PCIe GBE Family Controller, conectado a la máquina anfitriona por adaptador puente.

Las características de la máquina anfitriona son las siguientes:

- Procesador: CPU Intel(R) Core(TM) i7-2600K a 3.40GHz.
- Memoria RAM: 16 GB.
- Sistema Operativo: Windows 10 Pro (64 bits).

La versión de WhatsApp utilizada para todas las pruebas es la 2.16.366.

Desarrollo de las pruebas

Para la realización de las pruebas se ha utilizado la aplicación WhatsappScan, descrita en la Sección 3. Como se ha explicado con anterioridad, esta aplicación permite escanear un rango de números de teléfono determinado y obtener, de cada número, su estado, la fecha en la que lo actualizó, la imagen que tiene como avatar y la fecha en la que la añadió, siempre y cuando el número escaneado tenga una cuenta de WhatsApp y mantenga su estado y su avatar visibles o con algún contenido. Si se realizan varios escaneos del mismo rango y alguno de estos datos ha cambiado para algún usuario, se van añadiendo a su historial, permitiendo generar el historial de cambios asociados a cada usuario.

Se ha decidido realizar las pruebas dentro del rango de números de teléfono que comienza por 0034606. Las cifras 0034 son el prefijo de todos los números de teléfono españoles. Dentro de ellos, se ha decidido estudiar la franja que empieza por 606, ya que contiene algunos de los primeros números que se asignaron en España para telefonía GSM y es razonable que haya una gran cantidad de números activos en ese rango.

Se han realizado escaneos de mil números cada uno y, con la ayuda de la funcionalidad de grabación de eventos, se ha automatizando la tarea para que los escaneos se realizaran en bucle durante varios días. Cada escaneo de mil contactos ha tenido una duración de 36 minutos aproximadamente. En total se han tardado 15 días para escanear 500.000 usuarios, incluyendo las pausas para la recopilación de datos.

En las Tablas 7 y 8 se pueden observar los resultados obtenidos en cada prueba, en rangos de 100.000 contactos cada uno.

Tras obtener la base de datos "spy.db" descrita en la Sección 3, hemos realizado la siguiente consulta para obtener el número de usuarios que mantienen el estado por defecto: *select * from spy_status where status = "Hey there! I am using WhatsApp."* Los resultados obtenidos se pueden observar en la Tabla 9, donde los porcentajes mostrados se han calculado respecto al número de usuarios cuyo estado es visible.

Rango	Usuarios Whatsapp	Estados visibles	Fotos visibles
6060X	56.872	44.520	23.632
6061X	59.878	46.666	21.024
6062X	56.255	43.749	27.325
6063X	58.548	47.510	29.085
6064X	42.149	34.219	26.746
Total	273.702	216.664	127.812

Tabla 7. Resultados en unidades.

Rango	Usuarios Whatsapp	Estados visibles	Fotos visibles
6060X	56, 87	78, 28	41, 55
6061X	59, 87	77, 93	35, 11
6062X	56, 25	77, 77	48, 57
6063X	58, 54	81, 14	49, 67
6064X	42, 15	81, 18	63, 45
Total	54, 74	79, 16	46, 69

Tabla 8. Resultados en porcentajes.

Rango	Unidades	Porcentajes
6060X	10.888	24, 45
6061X	11.483	24, 60
6062X	10.523	24, 05
6063X	11.542	24, 29
6064X	8.339	24, 37
Total	52.775	24, 35

Tabla 9. Estados por defecto.

5. CONCLUSIONES

Una de las primeras conclusiones que podemos obtener tras las pruebas desarrolladas es que WhatsApp no ofrece ninguna protección frente a la sincronización masiva de nuevos contactos,

ya que hemos podido sincronizar y escanear medio millón de contactos sin dificultad.

Observando los resultados de las Tablas 7 y 8, se puede resaltar que se ha podido obtener información de un total de 273.702 cuentas de WhatsApp, que representan un 54,74 % de los teléfonos escaneados, lo que demuestra la gran popularidad de esta aplicación de mensajería instantánea en España. En la práctica, este porcentaje es incluso mayor, ya que actualmente no es posible identificar cuántos de los números de teléfono que carecen de cuenta de WhatsApp son líneas de activas o no, de ahí la elección del rango de números de trabajo realizada con el objetivo de minimizar la cantidad de líneas no asignadas a ningún usuario.

A su vez, se han obtenido 216.664 estados, pudiéndose afirmar que un 79,16 % de los usuarios tiene un estado visible y, de ellos, más de un 24 % mantienen el estado por defecto, como se puede observar en la Tabla 9. También se puede destacar que se han obtenido 127.812 fotos de avatar y que estas son las imágenes asociadas a un 46,69 % de los usuarios escaneados. En resumen, se pone de manifiesto que una gran cantidad de usuarios no restringe el acceso a su estado o imagen de avatar.

A la vista de los resultados obtenidos, se sugieren algunas medidas para mejorar la privacidad de WhatsApp, como sería implementar una configuración de privacidad por defecto más restrictiva, incorporar alguna limitación en la sincronización masiva de los contactos o integrar una identificación de usuario más segura.

Para terminar, es importante mencionar que el 20 de febrero de 2017 se produjo una actualización de WhatsApp con la versión 2.17.76 que introdujo un cambio en la funcionalidad relacionada con los estados. A partir de ese momento, los estados se caracterizan por ser imágenes o vídeos y dejan de ser exclusivamente cadenas de texto o emoticonos, como venían siendo en los últimos años. Estos nuevos estados tienen una duración de 24 horas y unas opciones de privacidad específicas, pudiéndose elegir entre qué contactos se desea compartir el estado. Desaparece la opción de "todos" (que implicaba mostrar a todos los usuarios) de las opciones de privacidad del estado, pero se mantienen en el menú las opciones asociadas al avatar y a la última hora de conexión.

Por todo ello, se planea ampliar esta investigación en el futuro, incluyendo en el análisis rangos de usuarios más amplios, incluso extendiendo el estudio a clientes de WhatsApp de otros países, adaptando al mismo tiempo la aplicación a los cambios que WhatsApps pueda seguir realizando. También se estudiará si es posible trasladar este ensayo a otras aplicaciones de mensajería instantánea.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente subvencionado por la Comunidad de Madrid (España), bajo el proyecto S2013/ICE-3095-CM (CIBERDINE) y por el Ministerio de Economía y Competitividad (España) bajo el proyecto TIN2014-55325-C2-1-R (ProCriCiS), cofinanciados con fondos FEDER.

REFERENCIAS

[1] Apple Inc., "iPhone premieres this Friday night at Apple Retail Stores," 2007, http://www.apple.com/pr/library/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores.html/.

[2] K. German, "A brief history of Android phones," 2011, https://www.cnet.com/news/a-brief-history-of-android-phones/.

[3] Pew Research Center, "Smartphones are more common in Europe, U.S., less so in developing countries," 2016, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

[4] Mobile Ecosystem Forum, "Mobile messaging report 2016," 2016, http://mobileecosystemforum.com/mobile-messaging-report-2016/.

[5] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 1:1–1:16. [Online]. Available: http://doi.acm.org/10.1145/2335356.2335358

[6] S. Schrittwieser, P. Fruhwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. Weippl, "Guess who's texting you? Evaluating the security of smartphone messaging applications," 2012. [Online]. Available: http://www.internetsociety.org/sites/default/files/07_1.pdf

[7] M. Terpstra, "WhatsApp & privacy," 2013. [Online]. Available: https://www.cs.ru.nl/bachelorscripties/2013/Martijn_Terpstra__0814962___WhatsApp_and_privacy.pdf

[8] N. Rastogi and J. A. Hendler, "WhatsApp security and role of metadata in preserving privacy," *CoRR*, vol. abs/1701.06817, 2017. [Online]. Available: http://arxiv.org/abs/1701.06817

[9] E. Kim, K. Park, H. Kim, and J. Song, "Design and analysis of enumeration attacks on finding friends with phone numbers: A case study with KakaoTalk," *Computers & Security*, vol. 52, pp. 267 – 275, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000589

[10] WhatsApp Inc., "One billion," 2016, https://blog.whatsapp.com/616/One-billion.

[11] Technopedia Inc., "Whats is an over-the-top application (OTT)?" 2017, https://www.techopedia.com/definition/29145/over-the-top-application-ott/.

[12] LINE Corporation, "line.me," 2017, LINE: Llamadasymensajesgratis/.

[13] PageBites, Inc., "imo.im," 2016, https://imo.im/.

[14] BlackBerry, "Acerca de BBM," 2016, https://www.bbm.com/es/about.html.

[15] Tencent Inc., "WeChat - free messaging and calling app," 2017, https://www.wechat.com/.

[16] Facebook, "1 billion people are on Messenger," 2016, https://messengerplatform.fb.com/.

[17] J. Schwartz, "The most popular messaging app in every country," 2016, https://www.similarweb.com/blog/worldwide-messaging-apps.

[18] WhatsApp Inc., "About WhatsApp," 2017, https://www.whatsapp.com/about/.

[19] Open Whisper Systems, "Video calls for Signal now in public beta," 2017, https://whispersystems.org/blog/signal-video-calls-beta/.

[20] Telegram, "Faq for the technically inclined," 2017, https://core.telegram.org/techfaq.

[21] Open Whisper Systems, "Open Whisper Systems home page," 2016, https://whispersystems.org/.

[22] C. Ballinger, "What is ChatSecure?" 2014, https://chatsecure.org/.

[23] Wickr Inc., "Securely connecting the word," 2017, https://www.wickr.com/security.

[24] Threema GmbH, "Threema cryptography whitepaper," 2017, https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf.

[25] WhatsApp Inc., "End-to-end encryption," 2016, https://blog.whatsapp.com/10000618/end-to-end-encryption?

[26] ——, "What is the 'verify security code' screen in the contact info screen?" 2016, https://www.whatsapp.com/faq/en/general/28030015.

[27] ——, "WhatsApp privacy policy," 2016, https://www.whatsapp.com/legal/#privacy-policy.

[28] DesdeLinux, "Como extraer respaldo de WhatsApp en GoogleDrive desde la consola," 2016, http://blog.desdelinux.net/como-extraer-respaldo-de-whatsapp-en-google-drive/.

[29] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digital Investigation*, vol. 11, no. 3, pp. 201 – 213, 2014.

[30] TzuTa Lin, "adb-event-record," 2016, https://github.com/tzutalin/adb-event-record/.