Universidad Nacional Autónoma de México

Facultad de Ingeniería

Cómputo móvil

Radiografía de una app

Signal

Alumnos	
Anaya Ruíz Yair Alejandro Jimenez Ruiz Gustavo Alfredo Santander Martinez Ángel Antonio	
Profesor	
Ing. Marduk Pérez de Lara Dominguez	
Fecha de entrega: 23 de octubre del 2021	**Grupo: 02**

Introducción

En este trabajo se realizará el análisis de la aplicación Signal. Esta aplicación fue creada como la unión de dos servicios de código abierto desarrollados por la compañía de seguridad móvil Whisper Systems, que fue fundada en 2010 por el investigador de seguridad Moxie Marlinspike y el desarrollador Stuart Anderson. Esta compañía lanzó los servicios de TextSecure para enviar mensajes de texto y RedPhone para realizar llamadas de voz en el sistema operativo Android, utilizando en ambas una tecnología de comunicación con cifrado de extremo a extremo. En noviembre del 2011 anunciaron que Twitter había comprado su empresa y decidieron hacerla de código abierto, en 2013 fundaron el proyecto de código abierto Open Whisper Systems (Lumb, 2018).

El primer proyecto que se realizó bajo el proyecto Open Whisper System, fue la creación de un protocolo, el protocolo Signal, que utiliza un método de encriptamiento que proporciona cifrado de extremo a extremo. En 29 de julio del 2014 se lanzó Signal para iOS como la contraparte de RedPhone y finalmente en noviembre del 2015 la aplicación RedPhone es unida a TextSecure y es renombrada como Signal para el sistema operativo Android (Greenberg, 2015).

El objetivo de la aplicación Signal es que cualquier persona, el público en general, pueda tener comunicación privada de manera gratuita, de acuerdo con palabras de uno de los fundadores, Moxie Marlinspike, “estamos tratando de hacer las comunicaciones privadas disponibles y accesibles como cualquier otra llamada normal por teléfono”, además Signal es descrita como una aplicación unificada gratuita, sencilla, de código abierto, que proporciona llamadas de voz y mensajería de textos privados (Greenberg, 2015).

Figura 1: Logo de Signal (Signal Messenger, 2020).

Antes de su creación, ya existían otras aplicaciones con el mismo uso de intercambio de mensajes, éstas implementan la forma de comunicación entre personas por medio de internet, ofrecen envío de mensajes de texto, videollamadas, llamadas y envío de archivos de manera gratuita, siempre y cuando se cuente con una conexión. Sin embargo, llegó a la sociedad para generar conciencia suficiente de la privacidad de los datos de las personas y la confidencialidad que éstas requieren.

La aplicación se encuentra dirigida al público en general que busca la comunicación vía internet. No importando la ubicación, raza y edad, el único requerimiento es contar con un número de celular. Signal es una aplicación utilizada en todo el mundo, sin embargo, se encuentra bloqueada en algunos países del medio oriente.

Descripción de la aplicación

Esta aplicación tiene la capacidad de detectar los contactos que utilizan también la aplicación y los muestra para poder comunicarse con ellos. Dentro de las conversaciones se pueden realizar videollamadas, llamadas de voz, enviar audios, enviar fotos, o mandar GIFs, archivos, contactos o la ubicación. Además, manda notificaciones de mensajes nuevos, se pueden crear grupos, se puede personalizar la apariencia de la aplicación, posee cifrado extremo a extremo de información con su protocolo de cifrado Open Whisper Systems, transferencia de cuenta, aplicación de escritorio, hacer respaldos del chat, bloqueo de capturas de pantalla dentro de la aplicación y desbloqueo nativo de cada plataforma (El comercio. 2021).

Se ha convertido en una de las alternativas para mantenerse en contacto con amigos y familiares, además se puede utilizar como una forma de comunicación de negocios entre los usuarios. Por ser una organización sin fines de lucro, las personas que lo utilizan se sienten seguros en cuanto a la privacidad de sus datos.

Al contrario de otros competidores como Facebook y Telegram, Signal no es un negocio, por lo que realmente no tiene un modelo de ganancia en el sentido tradicional. Open Whisper Systems es un proyecto colectivo compuesto por voluntarios y un número creciente de contribuyentes, que a veces reciben donativos y subvenciones. Hasta ahora, se ha podido financiar sin problemas la infraestructura del servidor a través de este sistema.

A diferencia de otras apps de mensajería instantánea como WhatsApp, Signal vela por la privacidad de la información de sus usuarios, excluyendo la compra y venta de datos de los mismos, por lo cual creemos que sería interesante saber más de ella y así poder informar a otras personas de su existencia.

Las principales aplicaciones que compiten con Signal son WhatsApp y Telegram, la diferencia está en que nuestra información está segura y nuestros datos personales no se venden. Signal es OpenSource a diferencia de Whatsapp o Telegram, lo que permite a expertos en conocimiento averiguar qué es lo que hace el código fuente, manteniendo transparencia de lo que se está usando. También a diferencia de Whatsapp se puede utilizar la aplicación de escritorio sin que el dispositivo móvil se encuentre conectado a la red.

Las licencias que se utilizan para el desarrollo de Signal son las siguientes:

- Clientes: GPLv3 - Cuando hablamos de software libre, nos referimos a la libertad, no al precio. Las Licencias Públicas Generales están diseñadas para garantizar que tenga la libertad de distribuir copias de software gratuito (y cobrar por ellas si lo desea), que reciba el código fuente o pueda obtenerlo si lo desea, que podrá cambiar el software. o

utilizar partes de él en nuevos programas gratuitos, y que sepa que puede hacer estas cosas. Para proteger sus derechos, debemos evitar que otros le nieguen estos derechos o le pidan que los renuncie. Por lo tanto, tiene ciertas responsabilidades si distribuye copias del software o si lo modifica: responsabilidades de respetar la libertad de los demás (GNU, s. f.).

- Servidor: AGPLv3 - La GNU Affero General Public License es una licencia copyleft gratuita para software y otros tipos de trabajos, diseñada específicamente para garantizar la cooperación con la comunidad en el caso del software de servidor de red (GNU, 2007).

Se encuentra en las tiendas de aplicaciones de los diferentes SO como la PlayStore (Android igual o posterior a 4.4) y la AppStore (iOS igual o posterior a 11.1) de manera gratuita (Signal Support, s.f). Para la aplicación de escritorio se requiere: Windows 64 bits: 7, 8, 8.1 y 10, macOS 10.12 y superiores, distribuciones de 64 bits de Linux compatibles con paquetes APT, como Ubuntu o Debian.

Está aplicación está disponible para los dispositivos móviles que cuenten con los sistemas operativos Android y iOS. También existe la versión de escritorio, pero el usuario debe encontrarse logueado desde la aplicación de su smartphone.

Figura 2: Capturas de la aplicación ejecutándose en los clientes móviles (Signal, s. f.)

Su versión más reciente es la 5.24.16 en Android mientras que en IOS es la 5.22.1, en lo que va del año lleva más de 50, por lo que se puede decir que se actualiza constantemente. En cuanto a la aplicación de escritorio, ésta se encuentra en su versión 5.20.0.

Signal no se encuentra recabando dinero por parte de la aplicación, es mantenida a través de donaciones. En 2018 recibió $600K dls en donaciones, pero gastó $4M en el personal y la infraestructura, el co-fundador de Whatsapp Brian Actor otorgó a Signal un préstamo de $105M sin intereses (Curry, (2021).

El número de usuarios a lo largo de los años es el siguiente:

- Diciembre 2019: 0.5 millones
- Julio 2020: 3.5 millones
- Diciembre del 2020: 30 millones
- Enero 2021: 40 millones

En cuanto a las descargas que ha tenido, se cuenta con los siguientes datos:

- Mayo 2020: 11 millones
- Enero 2021: 41 millones
- Mayo 2021: 105 millones

De acuerdo con la Play Store la aplicación se ha descargado más de 50 millones de veces y considerando que en mayo de 2021 la aplicación reportó haber tenido 105 millones de descargas, se puede observar que posee una cantidad de descargas muy similar en la plataforma de Apple. La aplicación se encuentra desarrollada y publicada por Signal Foundation/Signal Messenger.

En AppStore tiene 20,300 valoraciones con 4.6 estrellas. Los comentarios son buenos, al parecer a la mayoría le parece una buena alternativa, sin embargo, aún cuenta con varios bugs como puede ser en la toma de fotos, grabación de voz, cierre inesperado de la aplicación, etc.

En la Play Store hay más de 1 millón de comentarios sobre la aplicación y tiene una valoración de 4.4 estrellas, en general los usuarios recomiendan la aplicación y resaltan lo seguros que se sienten utilizándola, pero también reportan que tiene varios bugs que provocan el cierre de la misma.

Como podemos observar, Signal ha tenido cierto éxito respecto a sus competidores, ya que invita a los usuarios a preocuparse por la privacidad de sus datos y sus características lo hacen confiable para este nicho. Sin embargo, es necesario reconocer sus ventajas y desventajas, a continuación se muestra el FODA de Signal de acuerdo a sus características en el mercado:

Fortalezas	Oportunidades
• Aplicación gratuita. • Modelo sin fines de lucro. • Confidencialidad de las conversaciones, protección de la privacidad. • Encriptación extremo a extremo. • Poder tecnológico, resolución de problemas (número creciente de usuarios, bloqueos políticos).	• Cambio de condiciones de uso como en Whatsapp/Facebook. • Número creciente de usuarios de teléfonos móviles. • Avance en cómputo tecnológico. • Está disponible en los sistemas operativos móviles más populares (Android y iOS).

• Recomendaciones de varias figuras públicas (como Elon Musk). • Funciones de borrado automático de mensajes. • Libre de anuncios. • Código abierto.	
Debilidades	**Amenazas**
• Bloqueo en países como Egipto e Irán. • Utilización por grupos peligrosos. • Peligro de phishing o fraude. • Falta de características únicas. • Falta de popularidad. • Se requiere de un número telefónico para utilizarlo. • No se puede utilizar sin internet a comparación de los sms.	• Mercado muy competitivo. • Fallas en el servicio de las aplicaciones. • Incertidumbre en la cantidad de donaciones.

Tecnología de la app

En el caso de los clientes móviles Signal es programada para ejecutarse de manera nativa utilizando los lenguajes de dichas plataformas, como son Java, C, y Kotlin para Android Objective-C y Swift para iOS. Sin embargo, para la aplicación de escritorio, el método que se sigue es el híbrido, a través de Electron mediante el lenguaje de programación Typescript que se traduce a Javascript y que funciona como una aplicación web portada a escritorio. También utiliza una biblioteca llamada libsignal-client programada en Rust que implementa el protocolo Signal y su algoritmo de encriptación AES-GCM-SIV, posiblemente es la API que utilicen todas las demás aplicaciones.

Aunque en esta aplicación es importante el cliente, la funcionalidad principal, que es la comunicación, se realiza a través de la infraestructura del servidor, la única forma de comunicarse con este servicio es a través de las conexiones de internet, por lo tanto para utilizar esta aplicación es indispensable contar con una conexión mediante Wifi o datos móviles. La aplicación Signal utiliza un servidor central que se encarga de implementar el criptosistema de clave pública. En los criptosistemas de llave pública se utilizan dos llaves, una pública y otra privada, la llave pública de un usuario se intercambia con todos los demás usuarios que van a

enviar mensajes con éste. El servidor central es el encargado de compartir estas llaves y mantenerlas sincronizadas entre los usuarios.

La segunda llave es privada y se utiliza para cifrar los mensajes que serán enviados a través de la red, en Signal esta llave se almacena de manera local en el dispositivo utilizando la base de datos SQlite con la extensión SQLCipher, la llave privada es cifrada utilizando el algoritmo AES-256 y esta permanece en el dispositivo del usuario sin ser enviada. Una vez que un mensaje llega a otro usuario este es capaz de descifrar el mensaje utilizando la llave pública que le fue compartida.

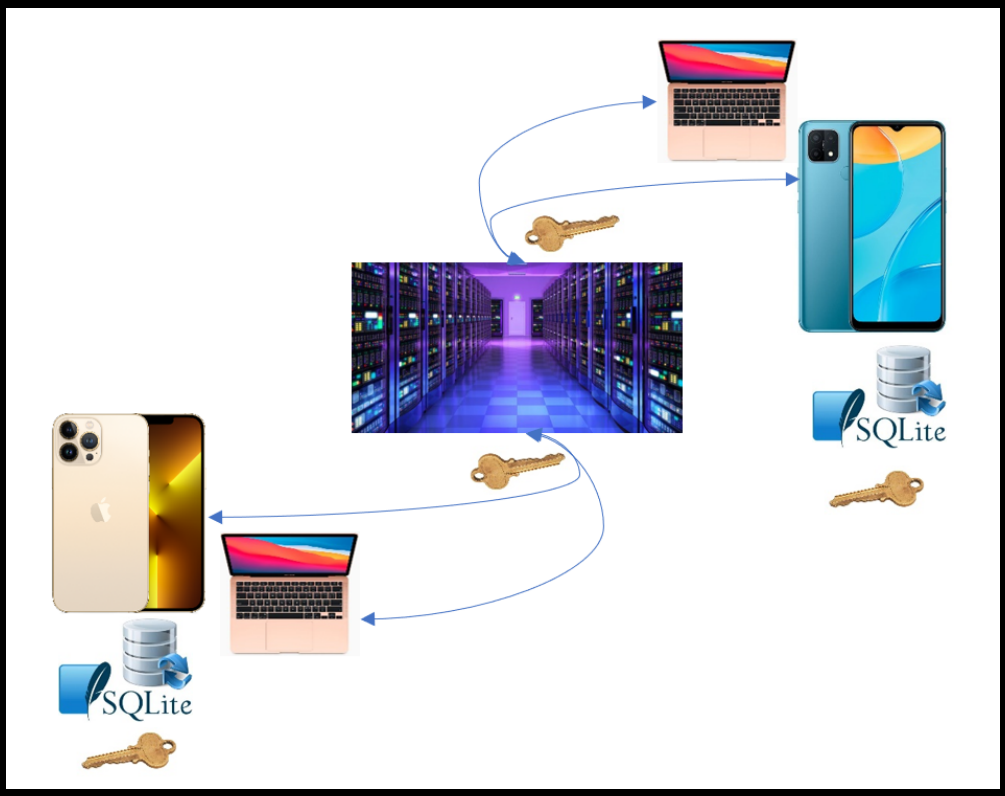

Figura 3: Esquema del funcionamiento del servicio de Signal.

Dentro de la aplicación del cliente se llevan a cabo todavía más acciones que le dan al usuario más características además de la seguridad que como se explicó anteriormente está cubierta por los servicios de backend. Signal permite acceder a la cámara para tomar fotografías y de esta manera enviarlas de una manera más cómoda, consideramos que no salir de la aplicación para realizar esta tarea mejora la experiencia de usuario. Otra característica que también es destacable, aunque está disponible en otros servicios, es la posibilidad de grabar mensajes de audio para enviarlos en la conversación de texto, por esta razón la aplicación pide permisos tanto para utilizar la cámara como para utilizar el micrófono.

La aplicación se conecta con otras aplicaciones instaladas en el dispositivo cuando requiere de enviar archivos del dispositivo, se pueden seleccionar desde cualquier aplicación de galería o de exploración de archivos que se encuentre instalada en el dispositivo.

En relación a la conectividad con otros dispositivos es posible utilizar relojes inteligentes para recibir notificaciones, a pesar de que no exista una aplicación para estos ya que es una característica de las plataformas en las que se encuentra disponible (iOS y Android).

Aún con todas estás características de la aplicación, consideramos que podrían agregarse algunas características que la diferencien de entre todos sus competidores, ya que como mostramos en el análisis FODA es un mercado muy competitivo, a continuación listamos algunas de ellas.

- Registro de una cuenta sin necesidad de contar con un número de teléfono
- Creación de canales
- Bots
- Canales de voz
- Capacidad para compartir pantalla
- Aplicación de escritorio nativa para un mayor performance
- Minijuegos dentro de la aplicación
- Permitir utilizar la misma cuenta Signal en distintos dispositivos móviles
- No mostrar la leyenda de que un mensaje fue eliminado
- Desvinculación de referencia de los mensajes eliminados
- Sincronización entre las bases de datos locales de los dispositivos

El número real de personal que intervienen en el equipo de desarrollo de la aplicación es muy variable ya que quien se encarga de modificar el código es la comunidad, sin embargo, consideramos que para realizar el mantenimiento de esta aplicación sería importante contar con lo siguiente:

- 5 project manager / product manager
- 20 diseñador UI/UX
- 25 iOS developer / 25 Android developer
- 25 backend developer
- 5 quality assurance engineer

Esta aplicación no posee un gran número de pantallas y de ellas el número de pantallas que son regularmente utilizadas son todavía menos. Como podemos observar en el diagrama la primera pantalla que aparece es la de bienvenida si es que el usuario no está logueado, en esta pantalla puede crear una una nueva cuenta, iniciar sesión o incluso transferir los datos de una cuenta de otro dispositivo al tiempo que se inicia sesión en uno nuevo.

Para iniciar sesión o crear una nueva cuenta se solicita el número de teléfono móvil y luego se envía un código por medio de sms que el usuario puede introducir de manera manual en caso de que la aplicación no la detecte automáticamente.

Una vez que se accede a la aplicación se puede observar el historial de conversaciones, desde donde se puede acceder a diferentes pantallas, al entrar a una conversación se puede enviar mensajes, hacer llamadas o enviar multimedia, adicionalmente se puede realizar la configuración de la conversación.

Finalmente de vuelta en la pantalla principal se puede acceder a la configuración general de la aplicación desde donde se tiene acceso a una gran cantidad de pantallas, las configuraciones disponibles son personalización de los colores de la aplicación, consultar los dispositivos en los que está activa la cuenta, realizar copias de seguridad, comprobar el espacio que ocupan los mensajes en el dispositivo, personalizar las notificaciones, bloquear contactos, bloquear las capturas de pantalla, evitar que los demás usuarios sepan cuando se leyeron sus mensajes o activar los mensajes temporales.

En la siguiente página se muestran las pantallas de la aplicación:

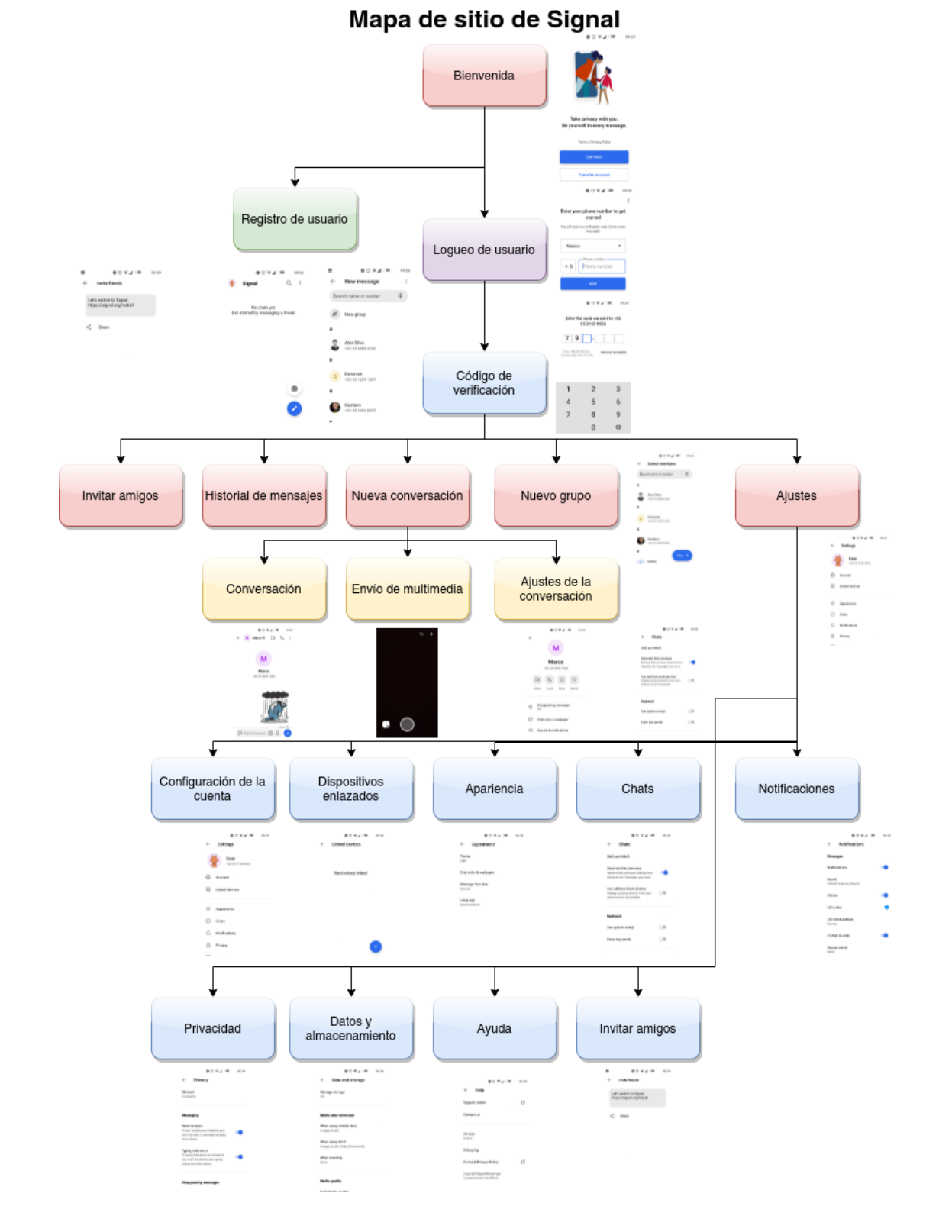

Figura 4. Mapa de sitio de Signal.

Popularidad y conflictos

Existen diversos reportajes donde se compara con su competencia directa WhatsApp, aludiendo su bajo nivel de caídas en la red, además de mejoras en las videollamadas ya que será capaz de ponernos en contacto, a la vez, con un total de 16 participantes.

Su popularidad ha ido creciendo constantemente, ya que 7.5 millones de usuarios se unieron a la plataforma en la segunda semana de enero, 43 veces más que la primera semana. Signal ha tenido algunas menciones que lo ha impulsado en popularidad, como la del magnate Elon Musk y su famoso tweet “Usen Signal” después de la caída masiva de Whatsapp a inicios de año.

Otras noticias importantes son aquellas donde se remarca su seguridad como una de las pocas aplicaciones de mensajería que no guarda la información de sus usuarios, por lo cual, es regularmente usada por periodistas e investigadores para proteger sus fuentes de información.

Algunos de los países en donde Signal es más usado son Egipto, Irán, Arabia Saudita y los Emiratos Árabes Unidos, sin embargo, algunos de ellos han tratado de bloquear la aplicación en su territorio, como fue el caso de Egipto en 2016, consiguiendo como respuesta por parte del grupo de la plataforma el agregar un frente de dominio a su servicio, permitiendo a los usuarios de Signal en un país específico eludir la censura haciendo que parezca que se están conectando a un servicio diferente basado en Internet. Otro caso similar al anterior fue en enero de 2018, cuando de igual manera fue bloqueada en Irán. Finalmente en enero de 2021, Irán eliminó la aplicación de las tiendas de aplicaciones y bloqueó Signal. Posteriormente, China bloqueó Signal en marzo de 2021.

Figura 5. Signal es bloqueado en varios países, incluido China.

En cuanto al uso criminal, al no poder leer los mensajes de los usuarios, excluye los intentos de moderación. Esto ha sido confirmado por auditorías independientes de los algoritmos de Signal. Esto se convierte, si pensamos en este benficio, en un arma de doble filo, tal como lo explicó la cadena de televisión CNN, "la misma tecnología que mantiene una conversación privada entre usted y un miembro de la familia también brinda un refugio seguro a un terrorista en Siria y a la persona en los Estados Unidos que está tratando de reclutar para cometer un acto de asesinato masivo", habiendo un caso similar en el año 2016, cuando las autoridades de la India arrestaron a miembros de una célula terrorista presuntamente afiliada a ISIS que se comunicaba a través de Signal y Telegram, otro caso fue la extrema derecha, las milicias de derecha y los nacionalistas blancos al utilizar Signal para organizar sus acciones, incluida la manifestación Unite the Right II en 2018.

Respecto a la tecnología que usa, sabemos que utiliza un protocolo de cifrado de extremo a extremo llamado Open Whispers Systems para todas las comunicaciones, lo que significa que los mensajes salientes de los dispositivos ya están cifrados y se descifran al entrar al dispositivo del receptor, todo lo contrario a sus apps competentes que hacen el cifrado durante el transcurso del envío de datos. Sin lugar a duda, la seguridad es su mayor fortaleza y la más importante al tratarse de comunicaciones, pues todo lo que queremos es que nadie invada nuestra privacidad y sepa de lo que hablamos con otras personas, sin embargo, esto como anteriormente se habló, podría ser un riesgo para los gobiernos que luchan contra la delincuencia cibernética y posibles actos de terrorismo, pues no hay forma en el mundo de ver lo que se habla en los chats.

Conclusiones

Con este análisis, sin duda alguna, conocimos mucho más de lo que sabíamos sobre los beneficios que nos brinda Signal y sobre todo sobre la seguridad que maneja en sus conversaciones, alentándonos a abrir nuestras cuentas y tal vez en un futuro cercano, recomendarlo a más personas y sepan que su privacidad será respetada sin ningún riesgo, siendo considerablemente mejor que aplicaciones como WhatsApp y Telegram, donde su principal negocio es la venta de nuestros datos y donde además de no haber privacidad, corremos el riesgo de ser interceptados por una persona mal intencionada y tenga acceso a nuestra información que suponemos es privada.

Desde el punto de vista de desarrolladores, estamos de acuerdo que la privacidad para los usuarios es primordial y más si se trata de una aplicación que está enfocada a la comunicación, sin embargo, encontramos algunos puntos que pueden ser preocupantes tanto a nivel personal como de estado. El primero lo es la forma de negocio que Signal utiliza, ya que se mantiene a gracias a donaciones que pudieran hacer los usuarios y al no haber venta de datos, no existe otra forma de conseguir alguna ganancia por el trabajo, si bien estamos totalmente cómodos en el tema de la privacidad, consideramos que tal vez se debería pagar por su uso, ya sea una cantidad mensual o única al adquirirla, pues por donaciones, a nuestro punto de vista, sería algo complicado seguir creciendo en nuevas aplicaciones o en el mantenimiento de la misma, tan solo el pensar que miles de personas están involucradas en su cuidado y actualización, así como servidores y distribución, suena complicado no tener un recurso monetario seguro. Por otro lado, está el que al ser una aplicación con cifrado Open Whispers Systems, claro está el riesgo del mal uso de Signal para organizaciones delictivas y que atentan contra el bienestar de una sociedad como los planes terroristas, incentivando cada vez más su uso para estas situaciones y en las que no podemos hacer mucho, pues se promete el mantener la privacidad de los usuarios, razón por la cual algunos países de Europa y Asia deciden bloquear y prohibir su distribución en los dispositivos inteligentes. Ante esto, no encontramos una solución eficaz y sin embargo sería algo que consideramos, la empresa fundadora debe prestar más atención, pues podría ser que al querer hacer un bien a la nación y mantener su privacidad como lo que es, esté ayudando a otros tantos con sus planes de odio y destrucción a ciertos grupos de personas vulnerables, no olvidemos que las vidas que cobra el terrorismo son inocentes y no directamante la de los involucrados en el gobierno por lo cuales se causan estos actos.

Referencias

1. Lumb, D. (2018, 1 noviembre). The story of Signal. Recuperado 22 de octubre de 2021, de https://increment.com/security/story-of-signal/

2. Greenberg, A. (2015, 3 noviembre). Signal, the Snowden-Approved Crypto App, Comes to Android. Recuperado 22 de octubre de 2021, de https://www.wired.com/2015/11/signals-snowden-approved-phone-crypto-app-comes-to-android/

3. El comercio. (2021, 11 enero). ¿Qué es Signal, cuáles son sus características y qué ventajas ofrece a los usuarios? Recuperado 22 de octubre de 2021, de https://elcomercio.pe/respuestas/whatsapp-que-es-signal-y-cuales-son-sus-caracteristicas-y-ventajas-mensajeria-instantanea-revlti-noticia/

4. GNU. (s. f.). The GNU General Public License v3.0 - GNU Project - Free Software Foundation. Recuperado 22 de octubre de 2021, de https://www.gnu.org/licenses/gpl-3.0.html

5. GNU. (2007, 19 noviembre). GNU Affero General Public License - GNU Project - Free Software Foundation. Recuperado 22 de octubre de 2021, de https://www.gnu.org/licenses/agpl-3.0.en.html

6. Signal Support. (s. f.). Security check. Recuperado 22 de octubre de 2021, de https://support.signal.org/hc/es/articles/360007211952-Soluci%C3%B3n-de-problemas-con-las-instalaciones-o-actualizaciones

7. Curry, D. (2021, 7 junio). Signal Revenue & Usage Statistics (2021). Recuperado 22 de octubre de 2021, de https://www.businessofapps.com/data/signal-statistics/

8. Signal Messenger. (2020, 2 junio). Logo of Signal [Ilustración]. Recuperado de https://upload.wikimedia.org/wikipedia/commons/6/6a/Signal-logo.png

9. Signal. (s. f.). Signal para dispositivos móviles [Ilustración]. Recuperado de https://signal.org/assets/screenshots/download-mobile-bdc14a52a345c02611f4a8ac2a2796dfd4f5f2d9cf9abbf2494bd3e244d63035.png

10. Varas, G. (2021, 17 marzo). Señal: la aplicación de mensajería está bloqueada en China. Logroño24horas. https://logrono24horas.com/senal-la-aplicacion-de-mensajeria-esta-bloqueada-en-china/