Artículo original

Las aplicaciones de mensajería instantáneas y la seguridad de la información en dispositivos móviles

Instant Messaging Apps and Information Security on Mobile Devices

Jeyson Prieto Collazo [1]*https://orcid.org/0009-0006-3079-7681
Félix R. Luzbet Gómez[2]* https://orcid.org/0000-0003-2719-8654

[1] Facultad de Matemática y Computación-Universidad de La Habana, Cuba.
[2] CEPES-Universidad de La Habana, Cuba.

*Autor para la correspondencia. felixrluzbetgomez@gmail.com

RESUMEN

El presente artículo formó parte de un estudio con alcance de maestría, en el cual se investigó lo referente a la valoración del esquema criptográfico del sistema de mensajería instantánea Signal, con énfasis en los fundamentos tecnológicos que lo sustentan. De igual forma, se evaluó su pertinencia en virtud de proponer y validar un esquema criptográfico seguro. En otro orden se esbozó el análisis de las principales aplicaciones de comunicación sincrónicas en dispositivos móviles y su clasificación a partir de los grupos de código abierto y de código cerrado, en cada caso se determinaron los principales factores estructurales que inciden y establecen su seguridad.
Palabras clave: Llaves criptográficas, esquemas criptográficos, seguridad informática.

ABSTRACT

This article was part of a master's study, in which the valuation of the cryptographic scheme of the Signal instant messaging system was investigated, with emphasis on the technological foundations that support it. Likewise, its relevance was evaluated by virtue of proposing and validating a secure cryptographic scheme**.** In another order, the analysis of the main synchronous communication applications on mobile devices and their classification based on the open source and closed source groups was outlined, in each case the main structural factors that affect and establish their security were determined.

Keywords: *Cryptographic keys, cryptographic schemes, computer security.*

Recibido: 5/2/2023
Aceptado: 5/5/2023

INTRODUCCIÓN

La historia demuestra que la forma de comunicarnos evoluciona progresivamente. El desarrollo de la ciencia y la tecnología diversifica dicho sistema comunicacional, que crea un flujo constante de información y mantiene a la sociedad inmersa en una paradoja circular, donde la confidencialidad, la integridad, la autenticación y el no repudio son elementos primordiales para establecer una comunicación segura.

Para garantizar estos aspectos es necesario implementar diferentes mecanismos, dentro de ellos los algoritmos criptográficos, los cuales utilizan técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no se puedan ser leer por aquellos usuarios que no estén autorizados para hacerlo.

DESARROLLO

En pleno auge de las comunicaciones digitales, la criptografía funciona como la base para cualquier proceso de seguridad informática; como son las aplicaciones de mensajería instantánea de nuestros dispositivos móviles, aplicaciones multiplataforma, o también servicios web. (Acoñac Prado, 2022)

Las diferentes aplicaciones móviles que existen para la comunicación, se clasifican en dos grupos: las de código abierto y de código propietario. Con la comprobación del código fuente de cada, en caso de que esté disponible para su análisis, se podrá determinar si las declaraciones de seguridad son ciertas.

Un software de código cerrado, común en proyectos que buscan monetizar su propiedad, por lo general, suelen tener puertas traseras, que se utilizan por los proveedores para acceder a la información de los usuarios, las cuales luego son expuestas a diferentes entidades como los servicios especiales de la inteligencia y empresas para enfocar sus mercados a ciertos grupos sociales.

Otros proyectos ponen su código fuente a disposición del público (código abierto); lo que permite mayores niveles de seguridad, ya que constantemente se exponen al escrutinio público, lo cual brinda oportunidad para que cualquier problema de seguridad o de otra naturaleza sea descubierto.

El análisis de las fuentes bibliográficas que se consultaron constató que concurren varios factores para determinar si una aplicación de mensajería es segura realmente y protege la privacidad de quienes la emplean; algunos de estos elementos a considerar son: **cifrado de extremo a extremo** que posibilita mantener la privacidad y seguridad de los datos durante su transmisión; pues se cifra el dispositivo del remitente y únicamente se descifra en el dispositivo del destinatario, así se evita que terceras personas intercepten y accedan a la información. De esta manera, incluso si alguien logra obtener los datos durante la transmisión, la información sigue siendo ininteligible para aquellos sin la clave de descifrado adecuada.

El software de código abierto, al permanecer disponible para el público de forma gratuita, permite que los beneficiarios puedan ver, modificar y distribuir ese código; lo cual influye en la generación grupal de mejoras y nuevas características.

La revisión de las **políticas de privacidad** es importante para comprender cómo se recopilan, almacenan y utilizan los datos personales. También es crucial para conocer si se comparten o venden estos datos a otras personas. Las aplicaciones almacenan de forma paralela datos sobre las conversaciones, tiempo de duración, dispositivos que se emplearon, las direcciones IP y los números telefónicos.

Los métodos **autenticación y control de acceso**, como contraseñas y autenticación a través de dos factores. Además, se deben gestionar controles adecuados para el acceso a la cuenta y su protección frente a ataques o intentos de robo de credenciales.

En los software se verifica el historial de **actualizaciones de seguridad** regulares que abordan y solucionan problemas que se identifican. Las actualizaciones son fundamentales para corregir vulnerabilidades y mejorar la seguridad.

De igual forma, es cardinal el establecimiento de medidas de seguridad integradas para la protección contra **malware y ataques**. Esto incluye la detección y bloqueo de archivos o enlaces maliciosos enviados a través de la aplicación y la **configuración y control de los niveles de privacidad, con especial énfasis a las personas que** pueden ver el perfil, quién agregar y contactar y qué información se comparte. Los **mensajes autodestruibles** se borran

automáticamente después de ser leídos o de un período de tiempo específico. Estos pueden ser enviados a través de aplicaciones o servicios en línea y son una forma de garantizar la privacidad y confidencialidad de la información compartida. Algunas plataformas permiten que el texto desaparezca solo del dispositivo del destinatario, mientras que otras pueden eliminarlo por completo de todos los dispositivos y servidores que se involucran.

La comprensión y contextualización de los factores que fueron expuestos, posibilita el análisis de la seguridad en las aplicaciones móviles de comunicación sincrónicas más relevantes, entre ellas a considerar:

- **Telegram**; Se creó por el emprendedor ruso Pavel Durov. La primera versión para Android y iOS data del año 2013 y ofrece las mismas funciones básicas, donde sus usuarios pueden enviarse escritos, stickers y archivos, crear grupos de conversación y realizar llamadas de voz.

Telegram utiliza el protocolo MTProto que se diseñó para acceder a un de servidor desde aplicaciones que se ejecutan en dispositivos móviles; a partir de algoritmos que se prueban en el tiempo para lograr que la seguridad sea compatible con la entrega de la información a alta velocidad y en conexiones débiles.

No obstante, Telegram solo cifra las llamadas de voz y las conversaciones secretas, para lo cual emplea un cifrado de extremo a extremo que según sus políticas de privacidad, al enviar y recibir textos no deja rastros en sus servidores, pueden ser autodestruidos y no permiten el reenvío de los mismos. Los chats comunes se cifran y se agrega un encabezado externo, como único identificador de clave de autorización para identificar tanto a personas como al servidor. Los archivos se almacenan en un servidor seguro que implementa su servicio en la “nube” y permite que se acceda a las conversaciones desde cualquier dispositivo.

Un punto crucial en cuanto a seguridad es la verificación del modelo de negocios de la aplicación, el cual está bien definido. En las configuraciones de la misma existe una opción para que los mensajes, archivos, fotos y los videos se autodestruyan al transcurrir un cierto tiempo desde su envío o recepción. Una vez que la información llega a su destino, permanece en el chat por un período configurable (entre un segundo y una semana) y luego desaparece. Igualmente, si se deja de usar la cuenta por determinado tiempo, fijado automáticamente en 6 meses, se borran los archivos multimedia, junto a todas las conversaciones guardadas.

En múltiples ocasiones y de forma sistemática, se ha puesto a prueba el esquema de cifrado de Telegram, en virtud de la identificación de vulnerabilidades y por consiguiente la revelación de los escritos; sin constar reportes de incidencias de esta índole.

- **Wire:** Se publicó por primera vez en 2014, por una empresa con sede en Suiza, como una aplicación de mensajería segura para Android, iOS, macOS, Windows y todos los navegadores populares; la cual fomenta el amparo de la información estadística y los datos de uso. Para su registro solo es necesario una dirección de correo electrónico y no el número telefónico. Precisamente, Suiza es un país que se considera de los más atractivos para cualquier servicio de interacción en los que prime la seguridad. Wire también ofrece cifrado de extremo a extremo, con carácter transparente, operando en segundo plano y en la configuración por defecto se encuentra activo. Su código es abierto; este se encuentra en los repositorios de GitHub y cualquier usuario puede acceder al mismo para analizarlo y realizarle controles de seguridad. En efecto, en diversos momentos ha sido auditado por especialistas ajenos a la empresa, los resultados de los procesos se publicaron en Internet; en todos los casos se ratificaron sus políticas de privacidad y el cumplimiento de las disposiciones del Reglamento General de Protección de Datos (RGPD).
- **WhatsApp:** Con más de 2000 millones de consumidores alrededor del mundo, es una de las aplicaciones de mensajería que más se utilizan. Fue de los primeros softwares en permitir una vía de comunicación segura a través del cifrado de extremo a extremo de manera predeterminada, no obstante, la adquisición por Facebook del registro de propiedad de la misma, ha puesto en dudas, el compromiso con la privacidad de la información en algunas personas,. En este sentido, si por algún motivo una conversación no está protegida, se envía una advertencia, lo cual posibilita que la comunicación sea cancelada de inmediato y no se guarde en los servidores de WhatsApp, si alguien logra acceder a los sistemas de la empresa, no podría descifrar las comunicaciones sostenidas, las cuales bajo una clave privada de cifrado, se conservan en un formato que permite crear, en Android y iOS, una copia de seguridad de los mismos y cargarla en la nube.

Otro elemento de importante es habilitar la verificación de la cuenta en dos pasos, mediante un PIN que verifique el número de teléfono en cualquier dispositivo que se emplee.

- **Threema:** Se desarrolla por tres jóvenes suizos con el nombre inicial de End-to-End Encrypted Messaging Application (EEEMA), luego las tres E se remplazaron por Three y quedó finalmente Threema. El nivel de anonimato que se emplea es elevado, porque a diferencia de lo

que ocurre en tantas otras aplicaciones, no se necesita usar un número de teléfono o una dirección de correo electrónico para abrir una cuenta. Threema permite enviar mensajes de voz y de texto, crear grupos, usar listas de distribución y hacer llamadas de voz y de video. El servicio no es gratuito, aunque sigue siendo de código abierto y cualquiera puede corroborar el cifrado de extremo a extremo. La empresa desarrolladora tiene como principio rector la prudencia en lo referente a los metadatos. Para evitar cualquier riesgo y que nadie pueda inmiscuirse en las conversaciones, los servidores de Threema las eliminan para siempre o son guardadas en el propio dispositivo del usuario. Producto a lo anterior, las comunicaciones no se pueden establecer por un canal que no esté cifrado y nadie las puede leer si no es uno de los participantes.

En contraposición a lo anterior se debe mencionar que no se permite la autenticación de dos factores.

- **Wickr:** Se crea en el año 2012 por un grupo de especialistas y expertos en privacidad y seguridad, para el establecimiento de conversaciones completamente anónimas. El servicio consta de distintas aplicaciones como AWS Wickr, AWS WickrGov, Wickr Me, Wickr Pro, Wickr ATAK Plugin, Wickr RAM y Wickr Enterprise. Cada una de ellas apunta a distintos grupos. La aplicación para uso personal es Wickr Me. Para registrarse en Wickr Me, no es necesario utilizar un número de teléfono o una dirección de correo electrónico; no se demanda esta información porque está pensada, precisamente, para no recopilar datos personales. Wickr se puede utilizar también para colaborar con otras personas, ya que permite compartir pantallas, ubicaciones y estados en línea.

La seguridad de Wickr se basa en utilizar el cifrado de extremo a extremo para todos la información, con la particularidad de cifrar cada documento que se envía en el dispositivo de origen utilizando una clave generada para ese en específico, por lo tanto, existen las claves necesarias para descifrar el contenido que se produce.

Además de cifrar las conversaciones y los datos, se eliminan los metadatos de todos los archivos que se transmiten a través de la red, de igual forma no almacena la información de las direcciones IP. A lo anterior se adiciona, que todos los beneficiarios de Wickr tienen acceso a informes de transparencia. También se emplea la autenticación de dos factores; es de código abierto, permite enviar mensajes autodestruibles, cuenta con una función para detectar capturas de pantalla y alguien escribe y se deja registrado en una captura de pantalla, se recibe una notificación.

- **Viber:** Surge como un software para la mensajería instantánea y de voz disponible en direcciones IP para varias plataformas. El derecho de autoría le pertenece a la multinacional japonesa Rakuten. En la actualidad prevalece en el mercado libre de costo, posibilita realizar llamadas gratuitas y enviar textos, fotos y videos. A través de Viber, es posible crear chats grupales de hasta 250 integrantes y realizar llamadas en conferencia con un límite de 20 participantes. En cuanto a seguridad, los mismos usuarios deciden el método de envío, cifrando las llamadas de voz y de video tanto en dispositivos móviles como en los principales sistemas operativos para equipos de escritorio. Tiene incorporado el cifrado de extremo a extremo en conversaciones individuales y en los chats grupales. Combina las conversaciones autodestruibles y ocultas, incluso con la opción de colocarles un pin secreto para su acceso.

Otras de las funciones importantes radican en las llamadas con número oculto, la visibilidad de estar en línea e incluso la confirmación de la lectura de los mensajes. En el software se presenta un esquema de colores para los diversos niveles de cifrado, en consonancia el color verde indica que la conversación está cifrada y que se está dialogando con una persona designada como confiable, el gris mantiene el cifrado, pero identifica a la persona como confiable y el rojo resalta que no se pudo autenticar el contacto.

- **Cyber Dust:** En el presente se denomina Dust; sus creadores indican en su sitio web que los archivos nunca se almacenan de manera permanente en ningún teléfono o servidor, además se pueden eliminar del teléfono del destinatario. Mantiene el cifrado de extremo a extremo, con la particularidad de que los escritos se autodestruyan en un plazo de 24 horas o apenas se lean. Otras opciones de privacidad lo constituyen las distribuciones de escritos a grupos de personas, pero que se leen en privado y el modo oculto en la denominación de los usuarios asociados a cada texto. Asimismo, se informan las capturas de pantalla y mediante un monitor de privacidad de conjunto con una herramienta de búsqueda, se puede incursionar en cualquier información en la Web de manera secreta.
- **iMessage**: Es un servicio de mensajería instantánea originado por Apple y presentado al público en 2011. Está disponible únicamente para las plataformas iOS, macOS, iPadOS y watchOS. Su cifrado es de extremo a extremo, limitando el tiempo para la visualización de fotos, videos o textos; solo en iOS 10 o versiones posteriores, regula la cantidad de veces que se puede acceder a ellos. Un aspecto de vulnerabilidad lo constituye la creación de copias de seguridad en

iCloud, que aunque posean claves controladas por Apple, exponen la información personal de miles de personas.

- **Line:** Conforma un sistema de comunicación seguro, libre de costo. Se fecha de producción se sitúa tras el tsunami que azotó a Japón en el año 2011. La catástrofe interrumpió muchos de los canales de comunicación estándar y condujo a Naver —una empresa de Internet— a buscar soluciones con el fin de que sus empleados se pudieran mantener en contacto. El producto originado, tuvo una fuerte acogida en su país de origen y, con el tiempo, fue ganando adeptos en otros países de Asia. Line ofrece cifrado de extremo a extremo, pero la persona debe indicar explícitamente que desea usar esa tecnología. El registro de uso requiere de la introducción del número de teléfono o sus credenciales de Facebook, aspecto que aumenta las posibilidades de usar los metadatos para crear publicidad dirigida.
- **Signal:** Es un programa de mensajería multiplataforma, destinado a llamadas de voz y textos cifrados de extremo a extremo. Es considerado por muchos especialistas como uno de los software de comunicación más seguros del mercado. Desde su presentación en el 2013, permite su acceso de manera gratuita y está disponible en los sistemas operativos Android y iOS. También posee una versión de escritorio para Windows, Mac y Linux. Quizás una debilidad en la aplicación se confirma en la autenticación a través de números telefónicos, sin embargo como su registro de propiedad no pertenece a una gran empresa tecnológica y su programación de código abierto se sustenta por subvenciones y donaciones, no contiene anuncios, afiliados ni seguimiento secreto.

Las conversaciones se cifran de forma predeterminada y son solo percibidas por los remitentes y receptores, también se eliminan de forma automática después de un tiempo establecido. Otros elementos a considerar es Signal no recopila demasiados datos personales y todo lo que se ubica en él se almacena únicamente en el teléfono de forma local. El protocolo de encriptación es tan fuerte, que incluso WhatsApp y Wire lo hace suyo para sus modos más seguros.

CONCLUSIONES

Al presente, la privacidad de la información es fundamental para garantizar la seguridad, proteger los derechos de las personas y su confianza en las tecnologías móviles. Como se aprecia existen disímiles protocolos para determinar la seguridad de las herramientas de comunicación en

dispositivos celulares. En cada una de ellas, las características y funciones de resguardo son diversas, por lo tanto los usuarios deben evaluar cuál es la que más se ajusta a sus intereses.

Es importante destacar que aunque se diseñen e implementen fuertes mecanismos criptográficos para evitar que la información se filtre, constan elementos como los errores humanos derivados de las interacciones en estas plataformas, que no se pueden descartar y que condicionan lo anteriormente expuesto.

REFERENCIAS BIBLIOGRÁFICAS

Acoñac Prado, S. (2022, 11 de noviembre). BLOGNEWS. Recuperado de https://cdes.es/blog/texto-y-mensajes-de-texto-definicion-y-ejemplos/

Alcántara, B. (2021, 14 de marzo). La Vanguardia. Recuperado de https://www.lavanguardia.com/andro4all/whatsapp/alternativas-seguras-whatsapp

Alcántara, B. (2023, 15 de enero). La Vanguardia. Recuperado de https://www.lavanguardia.com/andro4all/aplicaciones/que-fue-de-viper-la-app-de-llamadas-gratuitas-que-llego-a-competir-con-whatsapp

Borradaile, G. (s.f.). A la defensa del Disenso. Recuperado de Open Education Resources:https://open.oregonstate.education/defensadeldisenso/chapter/criptografia-moderna

Dust. (2019, 19 de enero). Recuperado de Declaraciones de privacidad de Dust: https://usedust.com/privacity-policy

Jiménez, J. (2023, 7 de marzo). Redeszone. Recuperado de https://www.redeszone.net/tutoriales/seguridad/usar-seguridad-aplicaciones-mensajeria-instantanea/^

Kaminsky, S. (2023, 8 de agosto). Kaspersky daily. Recuperado de https://www.kaspersky.es/blog/what-makes-a-messenger-secure/29048

Katzew, C. (2023, 18 de agosto). Rakuten Viper. Recuperado de https://www.viper.com/en/blog/2023-08-18/privacy-matters-viper-privacy-policies-updates-explained/

Ramírez, I. (2022, 20 de mayo). Xatakandroid. Recuperado de https://www.xatakandroid.com/listas/comparativa-a-fondo-aplicaciones-mensajeria-android-1

Conflictos de intereses

Los autores declaran que no existen conflictos de intereses.

Contribución autoral

JEYSON PRIETO COLLAZO: concibió la idea y elaboró el artículo.

FÉLIX R. LUZBET GÓMEZ: elaboró la introducción y aportó el sistema de parámetros para la caracterización de los sistemas de mensajería en dispositivos móviles.