Anderson Ramirez
Julian Gutierrez
Andres Gonzalez

¿Llega a ser WhatsApp lo suficientemente seguro como se piensa?

***Resumen*- Este texto analiza de manera general la situacion actual de la aplicación móvil WhatsApp, partiendo de la contextualización, pasando por los protocolos que usa, llegando a los objetivos que se pretenden con el desarrollo de la investigación, y terminando en lo que se hizo y se pudo comprobar de la vulnerabilidad en la plataforma web.**

***Abstract*- El propósito que se tiene al desarrollar la presenta investigación es ahondar un poco más en esos puntos débiles que presenta la red social WhatsApp y si es posible vulnerarlos con fines meramente académicos y de esta forma predicir que tan seguro puede llegar a ser el uso de este medio de comunicación.**

I. Introducción

Para nadie es un secreto que las redes sociales son hoy por hoy una parte fundamental para las personas, comunidades y la sociedad en general. Facotres como el exagerado crecimiento del contenido multimedia, la necesidad de estar conectado, comunicándonos, compartiendo, consumiendo, e interactuando con los demás durante la mayor parte del día son ejemplos de la cotidianidad a la que estamos acostumbrados por estos tiempos. Pero hasta que punto son seguras estas redes sociales a las que le confiamos desde datos personales, mensajes pivados, hasta cuentas bancarias. Preguntas como de que manera estas redes sociales garantizan la impenetrabilidad de hackers dentro de sus sistemas, son frecuentes en los usuarios que entregan información sensible a este tipo de plataformas. Por tal motivo muchas de las compañias propietarias de tales redes sociales, buscan la manera dia tras dia de mejorar sus sistemas de seguridad, con tan mala fortuna de que en algunos casos no logran abarcar la totalidad del asunto, por lo cual van dejando en el camino brechas denominadas vulnerabilidades, las cuales pueden llegar a ser explotadas con el fin de sacar beneficios personales y perjudicar a otros.

II. WhatsApp

Cuando hablamos de WhatsApp estamos refiriendonos a uno de los gigantes en redes sociales, ya que se encuentra dentro de la colección de aplicaciones de mensajería instantánea más usadas a nivel mundial, por lo tanto son millones de usuarios que a diario intercambian información por medio de esta red, desde texto plano hasta archivos de multimedia. Como todo sistema complejo en el mundo de las telecomunicaciones, require de un mantenimiento lo suficientemente sofisticado para garantizar a los usuarios un servicio de calidad y oportuno; no obstante este mantenimiento en teoría no llega a ser lo suficientemente completo, en particular si nos referimos a la seguridad del sistema, entendiéndose como la mínima posibilidad de que el servicio ofrecido sea manipulado por terceros y de alguna forma alterarse la vía regular en que se comporta el producto.

III. Objetivos del proyecto

Al igual que todo trabajo investigativo, poseemos una serie de objetivos que se pretenden alcanzar, y otros que por el momento no son factibles de conseguir. Dentro de los objetivos que se tienen presupuestados como alcanzables se encuentran:

- Identificar cuales son los puntos debiles que se presentan en el proceso de comunicacion dentro de la red social.
- Describir diferentes alternativas que se pueden llegar a usar para vulnerar la red social.
- Contrastar las vulnerabilidades de WhastsApp con otras aplicaciones moviles que posean una arquitectura similar.

Por otra parte, como objetivos que por el momento no son alcanzables se encuentran:

- Llevar a cabo un procedimiento similar al que se realizó con la red social WhatsApp para detectar posibles vulnerabilidades en otra red de mensajería
- Identificar si hay o no la existencia de un patrón general en las redes de mensajería instantánea para el cifrado e intercambio de la información.

IV. Metodologia

Para identificar el meollo de donde están lo posibles problemas primero se decidió entender la forma en que la red social estudiada garantizaba la seguridad de la comunicación entre usuarios de dicha aplicación, veáse sección V. De esta forma identificar los ya mencionados puntos débiles por los cuales se podría perpetrar algún tipo de ataque donde se viera comprometida la seguridad de la app, en este sentido se lograron identificar algunos y incursionar en uno de estos de manera práctica .

Hay que dejar en manifiesto que no en todas las vías identificadas la información del usuario se ve afectada en su totalidad, otras lo logran parcialmente donde sin

embargo si no existe la gestión adecuada para cubrir dichas brechas pueden llegar a ser causas de problemas de mayor grado en cuestiónes de integridad de la información del usuario.

V. WHATSAPP Y SU SEGURIDAD

WhatsApp intentando velar por la seguridad de la información que se intercambia entre los usuarios ha visto la necesidad de implementar métodos de encriptación cada vez más sofisticados, en la actualidad encontramos el cifrado punto a punto presente en cada aplicación móvil, que al ser un cifrado simétrico sólo existe la posibilidad de que al enviarse un mensaje se le asigna una llave o clave de encriptado y desencriptado que solo poseen tanto receptor como emisor, dichos mensajes se almacenan en una base de datos cifrada localmente, cabe destacar que el método usado para encriptar dichos mensajes está dado por medio del algoritmo AES-256 que lo hace a través de bloques de cifrado[1].

Todo lo anterior desarrollado durante esta sección es para mensajes de texto y multimedia en la red, sin embargo ¿Qué pasa con las llamadas, pueden ser potencialmente vulneradas?, la respuesta es aún poco clara en esta investigación debido a que el enfoque que se trató fue meramente de los protocolos y algortimos usados para la transmisión y cifrado de los mensajes depositados en las cajas de chat. No obstante la pregunta despierta curiosidad por lo que se deja como un objetivo a futuro ya que es un tema de donde se pueden desprender resultados críticos. Hasta ahora se sabe que WhatsApp para brindar seguridad en tiempo real a sus llamadas hace uso del recurso VOIP (Voice over internet protocol) [2] que podría ser considerado como un protocolo de seguridad que a su vez hace uso del protocolo SRTP que cifra de extremo a extremo lo que el flujo de streamings, todas estas tecnologías de cifrado se las provee la empresa Open System Whisper dueños de la red Signal.

Según WhatsApp los mensajes que son enviados de punto a punto son imposibles de desencriptar [3] incluso para las autoridades competentes más poderosas, así como el FBI, aseveran que los algoritmos utilizados son imposibles de vulnerar, tal vez sea cierto pero es importante aclarar que la principal deficiencia que puede presentar una red en cuanto a su seguridad muy probablemente existe dentro del canal usado para la transmisión de información en dicha red, que al usar algunos métodos no muy complejos se pueden llegar a interceptar y por ende a manipular.

Frecuentemente las aplicaciones de mensajería instantánea y de otro tipo de comunicación poseen sitios web para escritorio, de alguna manera se vuelve más tediosos llevar control sobre dos plataformas, y es esta una de las formas en que la red social WhatsApp devela una de sus principales debilidades en cuanto a su seguridad. De esta forma y en otras en el desarrollo de esta investigación y una vez conocida la forma en que la aplicación asegura la información se han identificado puntos débildes tales como:

- El más evidente, el intercambio de datos entre PC y móvil permite capturarar dicha información que llega a ser comprometedora
- La llave que permite descencriptar un mensaje está alojada localmente en los dispositivos móviles de cada uno de los usuarios
- La información como mensajes puede ser subida a repositorios en la nube, WhatsApp por ejemplo usa lo servicios de Google Drive
- Como se mencionó WhatsApp no usa tecnologías propias, de esta forma modificó unas cuantas líneas de los algoritmos que le provee Open System Whisper dejando una pequeña pero explotable ruptura a futuro.

Asi listamos las posibles siguientes vías de aprovecharse de dichas vulnerabilidades:

- Cambios en el código de cifrado
- Intercepción de la cryptokey y el msgstore
- Manipulación de mensajes a través de la web de WhatsApp

V.I CAMBIOS EN EL CÓDIGO DE CIFRADO

A muchos les ha pasado que se han visto en la necesidad o el lujo de adquirir un nuevo teléfono por lo que o bien la aplicación debe trasladarse de dispositivo o el usuario cambiar a un nuevo número, en ambos casos los mensajes que no se alcanzaron a leer presentan la posibilidad de recuperarse en el otro teléfono, esto se ve cuando aparece el mensaje "Esperando el mensaje. Esto puede tomar tiempo". La empresa informa que es debido al cifrado extremo a extremo ya que debe esperarse que el teléfono de quien envió el mensaje debe estar en línea para hacer efectiva ese cifrado [5]. ¿Pero que sucederá en ese lapso de “esperar” ese mensaje? Cabe la posibilidad de que ese mensaje se “pierda” en el ciberespacio como les puede haber ocurrido a muchos, estos mensajes de alguna forma podrían ser interceptados por alguna persona y leerlos, identificando esta vulnerabilidad como una de aquellas en las que el usuario se ve parcialmente afectado, ya que no se toma una conversación por completo [4].

V.II INTERCEPCIÓN DE LA CRYPTOKEY Y EL MSGSTORE

Como se mencionó anteriormente, en el dispositivo móvil de cada usuario se almacena una key con la cual se desencriptan los mensajes, dichos mensajes se encuentran alojados en una base de datos local encriptada, y solo dicha key la desencripta. Sin embargo dicha key no es visible para el usuario, pero eso no significa que no este ahí, y al poderse obtener es potencialmente comprometedor de una manera total, ya que si se llegará interceptar dicha key por parte de algún tercero entrometiéndose en el móvil de alguien directa o remotamente (métodos existen innumerables) este tendría acceso a todas las

conversaciones. La base de datos por su parte es totalmente visible para el usuario con la dirección /WhatsApp/Databases.

V.III Manipulación de mensajes a través de la web de WhatsApp

Como última pero no menos importante, de hecho es en la cual se ha decidido profundizar un poco más, encontramos dicha comunicación entre el sitio de escritorio y el móvil. Puede haber sido la menos pensada pero no hace más de 3 meses que se detecto la presente falla [6] en donde obteniendo una serie de parámetros se podía manipular el contenido de los mensajes de la aplicación WhatsApp, a la fecha esto aún es posible, simplemente extrayendo desde la herramienta de desarrolladores la llave pública y privada de la sesión de WhatsApp web antes de que el móvil escanée el código QR y a la vez teniendo al poder el parámetro secreto después de escaneado el código (esto mediante una captura de tráfico) para conocer variables del teléfono al cual se está accediendo.

En este sentido podemos hablar de las vulnerabilidades que presenta web whatsapp al dejar en manifiesto contenido que se puede desencriptar de una manera relativamente sencilla, aplicando ingeniería inversa a los algoritmos de encriptación. Cabe mencionar que whatsapp a la hora de serializar la información que se envía entre el dispositivo y el sitio web hace uso del protocolo protobuf2 protocol donde se almacena dicha información, no obstante su contenido puede deserializar

Al ingresar los parámetros anteriormente mencionados y con la ayuda de una herramienta como Burp Suite Professional y la extensión WhatsApp decoder se puede desencriptar el mensaje a texto plano, en el cual se pueden apreciar los siguientes parámetros:

-Conversación: este es el contenido real que se envía.
-Participante: este es el participante que realmente envió el contenido.
-fromMe: este parámetro indica si envié los datos o alguien más en el grupo.
-remoteJid: este parámetro indica a qué grupo / contacto se envían los datos.
-id: El id de los datos. La misma identificación aparecerá en las bases de datos del teléfono

La falencia es tan sencilla como cambiar el contenido de cada uno de esos parámetros. En este orden de ideas se presentan tres tipos de ataques que pueden realizarse aprovechándose de dichos cambios

V.III.I Cambiar la identidad de quien envia el mensaje

Esta vulnerabilidad se evidencia a la hora de enviar un mensaje por un grupo, cuando la victima envía el mensaje el atacante captura ese mensaje, lo desencripta (el proceso normal que se lleva a cabo para las demás vulnerabilidades) y después de eso se fija en el parámetro id, que como se explica es quien define quien envió un mensaje, simplemente puedo cambiar el contenido de dicho parámetro así Ej. –id:”cristian@whatsapp.com”, en ese momento el cambio ya esta efectuado después de enviado el mensaje, por lo tanto no está demás avisar que habría que responder a ese mensaje para que se vea el nuevo id de quien en “realidad” mandó aquel mensaje.

V.III.II Cambiar el contenido de un mensaje

Es la misma idea del proceso anterior, para este caso se aprovecha del contenido del parámetro conversation el cual una vez desencriptado se vería algo como asi Ej. –conversation: “Hola, como éstas?” (Mensaje original), podría ser modificado por “Hola, que tal?” y al igual que en el caso anterior se hace necesario replicar al mensaje para ver los cambios. Esto compromete crucialmente al usuario, podría ser usado con fines ilegales.

V.III.III Enviar un mensaje privado a través de un grupo

Este caso, no tan grave como el anterior, permite que un usuario envíe un mensaje a un grupo y simplemente cambiando el parámetro remoteId que es el id a quien va dirigido el mensaje ocultárselo a los demás miembros y solo el especificado en dicho parámetro sería quien estaría en capacidad de verlo.

Cabe destacar que los resultados al llevar a la práctica dichas vulnerabilidades fueron exitosos gracias a la herramientas antes descritas.

VI. Conclusiones

El proyecto de investigación se ha tornado bastante interesante, por lo que las posibilidades de que se siga indagando en el tema son muy probables. Lo que se concluye hasta el punto actual llega a ser satisfactorio en cuanto a lo aprendido, es imprensicindible conocer a cerca de como entre las capas de la arquitectura de la comunicación entre máquinas se intercambia la información, para estos casos fue curioso observar como el problema se extiende desde la capa de transporte a sus superiores como sesión y aplicación si nos referimos al modelo OSI. Estos nos llevó a establecer como objetivo contrastar el comportamiento de otras redes sociales con el de WhatsApp y identificar patrones específicos que hagan que estas redes de mensajería se vuelvan inseguras de alguna forma. A partir de esto se podría también tener en cuenta nuevas tecnologías que estén a la vanguardia en seguridad, WhatsApp claramente no lo es, también es oportuno reiterar que no hay sistema totalmente seguro pero si hay unos más seguros que otros, el primer paso estaría en darle la oportunidad a servicios de mensajería como Signal, Threema o Viber, entre otras. Así entonces se deja abierta la posibilidad de re tomar el presente proyecto para acaparar objetivos alcanzables en su totalidad, aasí como objetivos futuros.

REFERENCIAS

[1]https://es.wikipedia.org/wiki/Cifrado_por_bloques .Wikipedia
[2] Security protocols XXV (2017). Satajano Frank, Anderson Jonathan.
[3]https://faq.whatsapp.com/es/general/28030015/ . WhatsApp
[4]¿Confiable y seguro? (2018) Espinosa Ignacio, Guerra Carlos.
[5]https://faq.whatsapp.com/es/android/26000015/?category=5245250 .WhatsApp
[6]https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp/ (2018). Research CheckPoint.