# Vulnerabilidades en Whatsapp: Validez de los mensajes como prueba judicial

Recientemente, mi compañero Javier Rubio Alamillo publicaba en su página web un artículo en el cual ponía en entredicho la seguridad de la aplicación de mensajería Whatsapp y los mensajes almacenados en su base de datos, mostrando con sencillez la forma en la que estos podían ser manipulados.

Este artículo ha tenido mucha difusión en distintos medios y ha sido recogido con preocupación por abogados y miembros de la judicatura. Realmente no es para menos, el desconocimiento (que por otro lado es comprensible) de estos colectivos hacia la tecnología, hacía que, se aceptaran como pruebas capturas de pantalla de mensajes de whatsapp o incluso transcripciones de los mismos, como bien indicaba Javier Rubio en su artículo.

Indicar que este artículo no pretende en absoluto desacreditar o modificar las conclusiones del publicado por Javier Rubio, sino todo lo contrario, reforzar la conclusión del citado artículo: la necesidad de disponer de un perito informático con la debida titulación y conocimientos redacte un informe pericial, de cara a obtener pruebas que sean susceptibles de ser aportadas a procedimientos judiciales, con las debidas garantías.

Como comentamos, todo lo dicho por Javier en su artículo es cierto, pero creo necesario añadir algunos puntos. Si revisamos el artículo publicado se observa que el análisis y la modificación de la base de datos de Whatsapp se ha realizado sobre dos terminales que utilizan el sistema operativo Android. Existen distintos sistemas operativos para teléfonos móviles (Android, IOS de Apple, Blackberry, Windows Mobile, etc). No vamos a indicar que Android no es seguro y el resto sí lo son, ya que no es cierto. No existe absolutamente ningún sistema informático (sea un teléfono móvil o un ordenador) que sea totalmente seguro. Como indicaba el profesor universitario y experto en seguridad Gene Spafford "El único sistema totalmente seguro es el que está apagado, encerrado en un bloque de hormigón y protegido por guardias armados, y aun así tengo mis dudas". Pero si es cierto que existen sistemas que son más seguros o en su caso más difíciles de romper.

Por explicarlo de otra forma, la aplicación de Whatsapp y por consiguiente la base de datos que contiene sus mensajes, se encuentra ubicada dentro de un teléfono móvil. Para poder acceder al mismo y poder modificar los mensajes es necesario romper la seguridad del teléfono para acceder a su contenido. Es decir, es como si el teléfono fuera una caja fuerte que contiene la base de datos con los mensajes que se puede modificar. Ya no se trata tanto de la seguridad de la base de datos que Javier ha demostrado que es modificable, sino también de la seguridad del "recipiente" que la contiene. Y es fácil asumir que no todas las "cajas fuertes" tienen la misma seguridad.

En el caso de los teléfonos con sistema operativo Android, se ha podido constatar en numerosas ocasiones que su nivel de seguridad es bajo y actualmente, para muchos de sus terminales, es posible romper la seguridad del teléfono (abrir la caja fuerte), acceder a su contenido, modificarlo y volver a activar la seguridad del teléfono (cerrar la caja fuerte) sin dejar rastro (aunque esto requiere más conocimientos informáticos).

Otro tema distinto, sería en el caso de terminales Apple, su sistema operativo es mucho más robusto, aunque también es posible romper la seguridad del teléfono (abrir la caja fuerte). Pero esta apertura implica la "rotura de la cerradura", es decir, el perito que escribe este artículo no conoce un método para romper la seguridad del teléfono sin dejar rastro (actualmente en nuestro laboratorio estamos estudiando distintas alternativas sin éxito, pero además no hay garantías que estos métodos funcionen en todos los casos), una vez abierta la caja no se puede cerrar sin que quede constancia de la alteración. De esta forma, si nos enfrentamos a un peritaje de un teléfono Apple que no ha sido rota su seguridad (lo que se conoce técnicamente como Jailbreak), hay una alta probabilidad de que los mensajes que contiene este terminal no hayan sido alterados y puedan ser utilizados como evidencia cuando han sido verificados por un perito informático con la debida titulación y formación.

El mismo caso ocurre para terminales Blackberry, que a mi criterio son los más seguros (están más orientados a entornos profesionales) siendo más difícil (que no imposible) la modificación del contenido del teléfono, y en consecuencia la modificación de los mensajes alojados en una base de datos whatsapp.

Además y ya para concluir, hay que tener en cuenta la evolución de la tecnología. Hace muy poco tiempo whatsapp no existía, en sus inicios los mensajes no se cifraban, y actualmente sí -aunque se pueden descifrar-. No es atrevido afirmar que Watsapp puede con facilidad mejorar la seguridad de su aplicación para que en un futuro el acceso y modificación de estos contenidos sea mucho más difícil. Por ello es necesario el rol del perito informático, es el único profesional cualificado para analizar una evidencia electrónica y emitir un informe que le indique a un juez, abogado o cliente si se detecta indicios de manipulación o en su caso si ha sido posible esta manipulación sin dejar rastro.

Replicando las conclusiones de Javier Rubio "**WhatsApp es una aplicación muy poco segura y fácilmente manipulable**, por lo que la aceptación de conversaciones mantenidas a través de la misma como prueba en un juicio, debe realizarse con cautela y, por supuesto, siempre con el aval de un perito informático colegiado." No obstante hay que destacar que **no se debe inicialmente descartar la validez de los mensajes ya que hay que tener en cuenta otros factores como el terminal en el que están alojados o la evolución de la tecnología**, por lo que será necesario realizar un profundo y exhaustivo análisis forense para dictaminar si las conversaciones son o no auténticas.

Autor: Carlos Pintos Teigeiro
Informática y Peritaje
http://www.informaticayperitaje.com