Proyecto ELO-322

Maria Gabriela Castro Almendra 201530021-6
Nicholas Andreas Bernal Alvarez 201530010-0

Resumen

Nuestro proyecto consistió en averiguar sobre la arquitectura general de una de las aplicaciones de mensajería multiplataforma más utilizadas en mundo, whatsapp. Sin embargo, no nos bastó con tener solo la teoría y decidimos ponerlo a prueba, para también tener un punto de vista empírico de lo que leíamos.
Además de esto, averiguamos sobre los protocolos de la no tan reciente extensión para computador de whatsapp llamada “whatsapp web” la cual nos dimos cuenta por su manera de funcionar que no es tan óptima como creíamos.

Introducción

Considerando que la aplicación de mensajería multiplataforma, Whatsapp, es una de las más populares con un número superior a mil millones de descargas a nivel mundial y que en los últimos meses a dado bastante que hablar por sus recientes cambios respecto al cifrado de los mensajes y por ende la privacidad de sus usuarios, hemos decidido averiguar sobre sus protocolos y estructura de manera general para entender mejor cómo funcionaba antes y después del cifrado.

Arquitectura de whatsapp y funcionamiento de whatsapp web

Empezamos con la investigación recorriendo varias páginas de internet con información respecto a whatsapp y a extraer la información que considerábamos relevante al respecto.
Lo principal fueron los protocolos que utilizaba, una versión modificada y adaptada de XMPP llamada funXMPP.

¿Que es XMPP?

Es un protocolo abierto que se creó para ser usado en sistemas de mensajería instantánea, originalmente está basado en XML. En un principio se conocía como Jabber, y el proyecto fue iniciado en 1998 por Jeremie Miller.
Con el protocolo XMPP queda establecida una plataforma para el intercambio de datos XML que puede ser usada en aplicaciones de mensajería instantánea. De este modo, las características en cuanto a adaptabilidad y sencillez de XML las hereda el protocolo XMPP.

Diferencias entre XMPP y funXMPP

Caracteristicas de XMPP	'Lo eserado	Lo que Whatsapp hace/permite/prohibe
Atrubitos del cliente stream:stream nodos	Cualquier atributo, incluidos los espacios entre nombres	Exactamente 2: "to" y "resource"
caraterísticas de transmisión	cualquier característica usada durante la comunicación	Sólo `<receipt_acks />` (Ni siquiera SASL con todos sus mecanismos)
Mecanismos de SASL	Cualquiera de ellos, incluido "DIGEST-MD5"	Sólo "DIGEST-MD5" es soportado, el cual es (y deberia ser) llamado "DIGEST-MD5"
SASL succes	Se abre una nueva fuente reemplazando la anterior	Despues de `<success />` del mensaje, nada es enviado por el servidor
Varios inicios de sesion para una cuenta	Multiples usiarios usan distintos recursos	una coneccion reemplaza a la otra sin importar los recursos que utilice esta.

Mensajes de Whatsapp

El Jabber ID (JID) está compuesto por el número de teléfono que hemos registrado y el dominio s.whatsapp.net. El id del mensaje permite diferenciarlo de forma única del resto, así no habrá problemas con el procesado posterior. Como se muestra en la imagen:

```
<message from="01234567890@s.whatsapp.net"
         id="1339831077-7"
         type="chat"
         timestamp="1339848755">
    <notify xmlns="urn:xmpp:whatsapp"
            name="NcN" />
    <request xmlns="urn:xmpp:receipts" />
    <body>Hello</body>
</message>
```

Los campos mencionados anteriormente se ubican, en las primeras línea del código donde se ven claramente. Sin embargo se quiso optimizar el tamaño del mensaje cambiando los comando, o las palabras reservadas utilizada, por un byte así se aliviana mucho más el paquete. FunXMPP utiliza una tabla hash para la conversión de cifrado, con esta modalidad tenemos bytes de la forma:
\xnn (nn es un número hexadecimal), obteniendo:

```
<\x5d \x38="01234567890@\x8a"
      \x43="1339831077-7"
      \xa2="\x1b"
      \x9d="1339848755">
   <\x65 \xbd="\xae"
         \x61="NcN" />
   <\x83 \xbd="\xad" />
   <\x16>Hello</\x16>
</\x5d>
```

ENCRIPTADO DE EXTREMO A EXTREMO

Podemos decir que después de que Alemania tilda a whatsapp con inseguro y poco privado, y ahora con sus problemas en Brasil y su caso judicial en la policía de dicho país. Whatsapp parece tomar la opción de encriptar los mensajes de sus clientes de extremo a extremo, pasando de ser una aplicación insegura,a una con seguridad bastante grande.

¿Cómo es esto del cifrado de extremo a extremo?

Bueno, esto está basado en un protocolo llamado **Signal,** y funciona con el almacenamiento de las claves de encriptado y desencriptado, para poder descifrar el código en los respectivos dispositivos móviles, así el encriptado es en todo el viaje del paquete, de manera tal que ni el mismo proveedor de servicio pueda saber el contenido del mensaje.

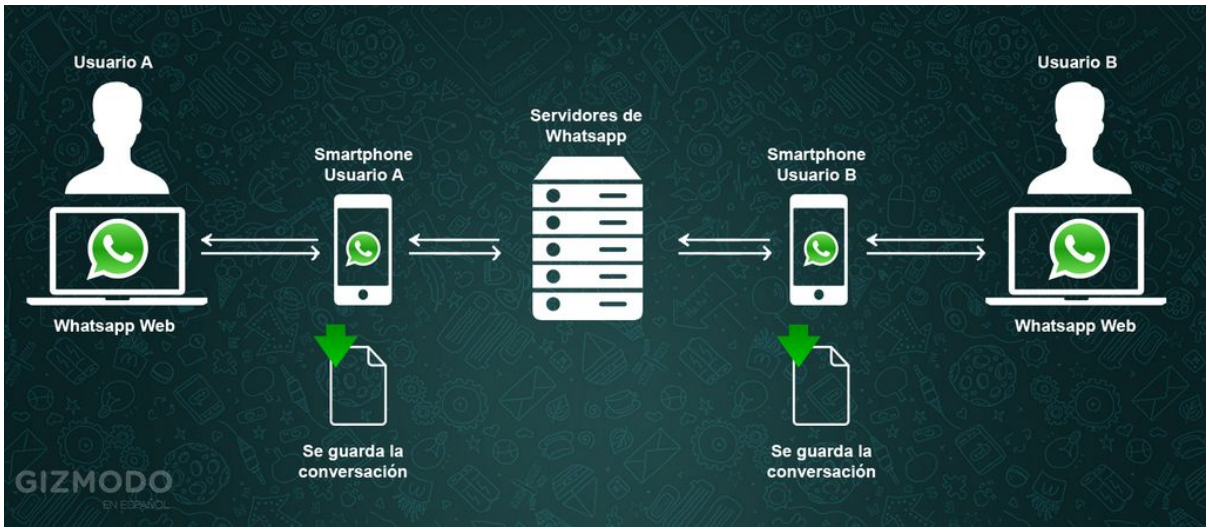
¿Cómo sucede esto?

Se generan 6 claves distintas, 3 públicas y 3 privadas:
Las públicas primero una para identificar el dispositivo; conservaría la id como clave, la que mencionamos anteriormente, otra se genera periódicamente y la cual es firmada digitalmente por la contraseña anterior, y por último una que solo se usa cuando se actualiza el servicio de whatsapp.
En cuanto a las privadas; la primera es una clave de administrador que se usa para generar una clave de cadena q se una para crear la clave de mensaje, y por último la clave de mensaje. Estas son las medidas de seguridad que no permiten, si no ha de ser el dispositivo receptor o emisor, codifica el mensaje enviado entre medio del viaje, a su vez estas contraseñas se van guardando en dichos móviles, lo que genera, que ni en los servidores podamos encontrar dato alguno del mensaje enviado, y mucho menos descifrarlo, dejando la posibilidad de ver el mensaje sólo si tenemos el terminal desbloqueado.

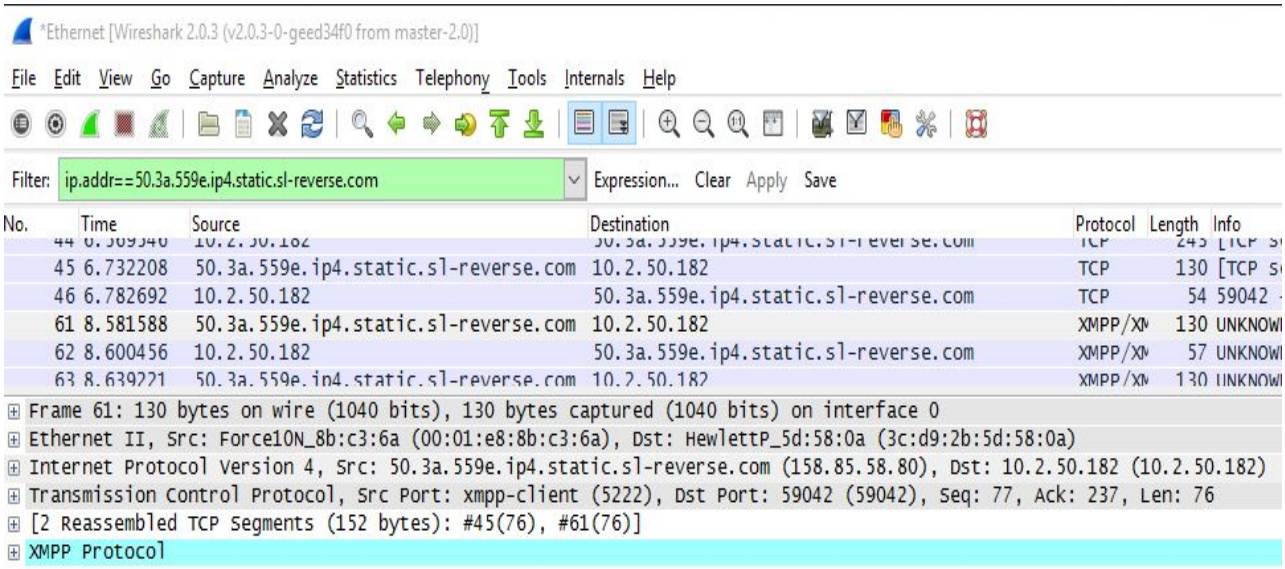
Whatsapp Web

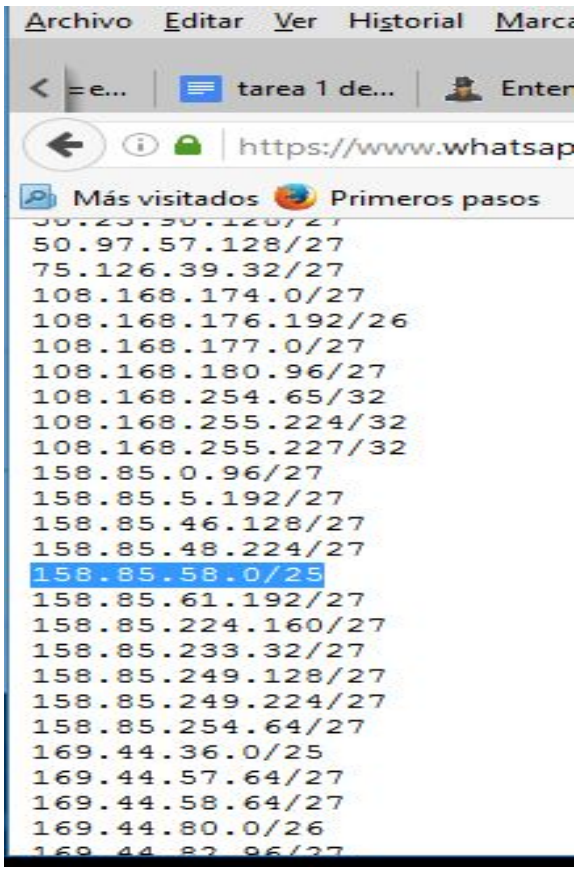
La aplicación Whatsapp Web es una extensión de whatsapp de dispositivos móviles para computadores, sin embargo esta aplicación es bastante ineficiente cuando la investigas un poco más a fondo. De manera sencilla, el asunto radica en la forma en que WhatsApp funciona como compañía, no almacenando en sus servidores los mensajes de sus usuarios. Esto implica que los mensajes sólo se alojan en dos lugares, el smatphone de la persona que envía y el smartphone de la persona que lo recibe. Cuando abrimos WhatsApp Web en el fondo lo que hacemos es sincronizar el computador con nuestro smartphone y recuperar directamente desde el teléfono los mensajes, por eso la aplicación no funciona si el smartphone se encuentra apagado o desconectado de la red.

El lado positivo de esta situación es que la privacidad de los usuarios es bastante alta, pues la aplicación no tiene un respaldo de los mensajes ni como acceder a ellos, ni siquiera un gobierno puede pedirle a la aplicación WhatsApp que entregue conversaciones privadas, básicamente porque whatsapp nos las tiene.



Resultados prácticos
podemos ver que hemos capturado los paquetes saliendo del pc, y vemos que las ip son 158.85.58.80.





podemos notar que la ip es parte de la subred de máscara 25, la ip mostrada en la foto.
por lo tanto podemos revisar que el mensaje está en el protocolo xmpp en la parte inferior de la captura, que demuestra a su vez que es realmente la dirección que buscamos

Conclusión

Luego de nuestra extensa investigación sobre la estructura de la aplicación de mensajería instantánea sobre la cual decidimos averiguar llegamos a varias conclusiones sobre los distintos puntos que explicamos en el desarrollo del proyecto.

-A pesar de haber recibido varias y fuertes críticas sobre su privacidad y su política de ciframiento de los mensajes, con las nuevas actualizaciones, Whatsapp se ha transformado en una de las aplicaciones de mensajería multiplataforma más segura del mercado.

Referencias

-http://mundotech.net/funcionamiento-de-whatsapp/
-https://hipertextual.com/archivo/2014/07/protocolo-xmpp/
-http://www.seguridadofensiva.com/2013/12/ntendiendo-el-protocolo-de-whatsapp-funxmpp.html
-http://es.gizmodo.com/como-funciona-la-chapuza-de-whatsapp-web-explicado-en-1681131120
-http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/Protocolo_XMPP.pdf
-https://github.com/mgp25/Chat-API/wiki/FunXMPP-Protocol
-https://www.whatsapp.com/cidr.txt