Redes de Computadores I

"OneDrive"

Integrantes: Javier Sanhueza
Macarena Sepúlveda

Profesor: Agustín González

Fecha: 28/09/2015

Índice

1. Resumen

Nubes virtuales: La nueva era del almacenamiento de datos. Indagaremos en una de las principales nubes virtuales, que es OneDrive, cuál es su competencia, sus pro y contras, pero principalmente ahondaremos en su protocolo de seguridad (TLS).

2. Introducción

Desde tiempos inmemorables la humanidad ha almacenado la información de una u otra forma, y ahora en la actualidad cuando poseemos tecnologías (tales como los notebooks, tablets, celulares, entre otros) preferimos almacenarlo en estas ya que es más fácil y rápido obtener la información guardada. Ahora bien, de esta forma, surge un inconveniente que es el que los aparatos tecnológicos no siempre los traemos con nosotros, o bien, se descargan. Entonces, cuando necesitamos este archivo, música, vídeo, etc. no podemos acceder a él hasta poder tener en nuestras manos y encendido el aparato tecnológico que lo contenía. Frente a este problema se idealizó un servicio donde la información se pudiera almacenar en la red y sacarse de ésta cuando fuera requerida, de cualquier aparato tecnológico que esté conectado a la cuenta del cliente. Esto, al igual que otras empresas, lo hace Microsoft con OneDrive.

3. OneDrive [1]

OneDrive es un servicio de alojamiento de archivos, propiedad de Microsoft, diseñado para almacenar contenido estático, mayormente grandes archivos que no sean páginas web, que no superen el TB de información (Puede ser música, fotos, vídeos, entre otros.).

3.1 Historia de OneDrive [1]

- 2006: Microsoft anunció la aparición de “Disco duro virtual”, que servía para almacenar información en internet.
- 2007, Mayo: Salen los primeros *testers (probadores de software) en USA.* El software es nombrado: **Windows Live Folders.**
- 2007, Agosto: Windows Live Folders cambió de nombre a **Windows Live SkyDrive**, y la prueba de este software se extendió a testers de India y Reino Unido. Con sus máximos 250 MB de almacenamiento, podía almacenar imágenes, documentos y música, dentro de una de las tres carpetas designadas (privado, sólo amigos, público).
- 2008, Mayo: Windows Live SkyDrive estaba disponible para 62 países, y la idea de las carpetas designadas fueron eliminadas. A la fecha, el almacenamiento disponible aumentó de 250 MB a 5GB.
- 2008, Agosto: SkiDrive aumento su capacidad a 25GB, de los cuales 5GB eran utilizados en ***Live Mesh*** *(*un sistema de sincronización de datos que permite a los archivos, carpetas y otros datos compartir y sincronizar múltiples dispositivos personales).
- 2011, Mayo: Microsoft creó una aplicación instalable para Windows y OS X. Recuperó los 5GB utilizados en Live Mesch.
- 2014, Febrero: Cambia de nombre a **OneDrive.**

3.2 Ventajas de OneDrive [3]

- Da seguridad, puesto que necesitas una contraseña para ingresar, y además con los protocolos que posee (que se verán más adelante) a cualquier Mitm (Man in the middle) que deseara robar la información le sería más difícil desencriptar los contenidos.
- Su utilización es sencilla, y subir y descargar los archivos es algo totalmente fácil para cualquiera.
- Es compatible con celulares Android, IOS y Window Phone.
- Está ligado con Office, muy factible para aquellos que usan estas aplicaciones con frecuencia.

- Posee una capacidad inicial de 15GB y se puede ampliar a 200GB.
- Es más económico con respecto con sus competidores
- Una vez abierto un archivo no se necesita conexión para requerirlo.

3.3 Desventajas de OneDrive

- Limita el tamaño del archivo que se desea subir, éste puede pesar como máximo 300 MB.
- Cuenta con GB gratis, pero para aumentarlo hay que pagar.
- Agencia de seguridad nacional estadounidense, tiene acceso a todos los contenidos.
- Para usar OneDrive se necesita una cuenta Microsoft.

4. Comparación con otras nubes virtuales

Para ver si OneDrive es realmente conveniente, hay que hacer una comparación de sus características con sus principales competidores [2].

	DROPBOX	GOOGLE	MICROSOFT	APPLE
Espacio gratuito	2 Gb.	15 Gb.	15 Gb.	5 Gb.
100 Gb.	-	1,99 $ / mes	1,99 € / mes	-
200 Gb.	-	-	-	3,99 $ / mes ***
1 Tb.	9,99 € / mes	9,99 $ / mes	2 € / mes *	-
Seguridad				
Cifrado	AES 256 bits	HTTPS / TLS	PFS	AES 128 bit
2 pasos	Sí	Sí	Sí	Sí
SSOO				
Android	Sí	Sí	Sí	No
iOS	Sí	Sí	Sí	Sí
Windows Phone	Sí	No **	Sí	Sí
Mac OS	Sí	Sí	Sí	Sí
Windows	Sí	Sí	Sí	Sí

Cabe mencionar su seguridad en cifrado PFS que es una de las mejores existente en el mercado [3] y el significado de la verificación 2 pasos: herramienta que hace más difícil entrar a nuestra nube virtual para algún agente sospechoso, porque a parte de nuestra contraseña, manda un código al teléfono celular ya sea una mensaje de texto, llamada o usar el celular como USB llave de seguridad.

5. Protocolos que OneDrive utiliza:

5.1 TCP: Es uno de los protocolos fundamentales de la redes de computadores, ya que su función principal es que dos host puedan establecer conexión e intercambiar datos, de forma garantizada, es decir, que ningún dato se pierda durante la transmisión, y que los paquetes sean recibidos en el mismo orden en que fueron enviados.

5.2 Transport Layer Security (TLS) [4]**:** en español seguridad de la capa de transporte son protocolos criptográficos que protegen la conexión entre servidor web y cliente.
Este protocolo se divide en 2 sub-protocolos:

I) Protocolo de registro: Permite que los datos protegidos sean convenientemente codificados por el emisor e interpretados por el receptor.

II) Protocolo de negociación (Hanshake Protocol): Tiene como propósito autenticar al cliente y servidor, acordar los algoritmos de codificado y claves que se utilizaran de forma segura.

En esta parte se pueden apreciar 10 mensajes (depende de la conexión) de intercambio entre servidor y cliente:

1) Hello Requet: El servidor espera que el cliente inicie negociación, si no es así el servidor envía un hello request.

2) Cliente Hello: Cliente inicia la conexión, mandando una lista de combinaciones de algoritmos criptográficos que el cliente ofrece, el algoritmo de MAC, etc.

3) Server Hello: Repuesta del servidor a nuestra petición.

4) Cerficate o Server Key Exchange: Servidor se autentifica al cliente o intercambio de claves de parte del servidor.

5) Certicate Request: el servidor pide una autentificación al cliente (si es que es necesario).

6) Server Hello Done: Para terminar esta primera fase de diálogo.

7) Certificate: Cliente se autentifica al servidor.

8) Client Key Exchange: Intercambio de claves del cliente.

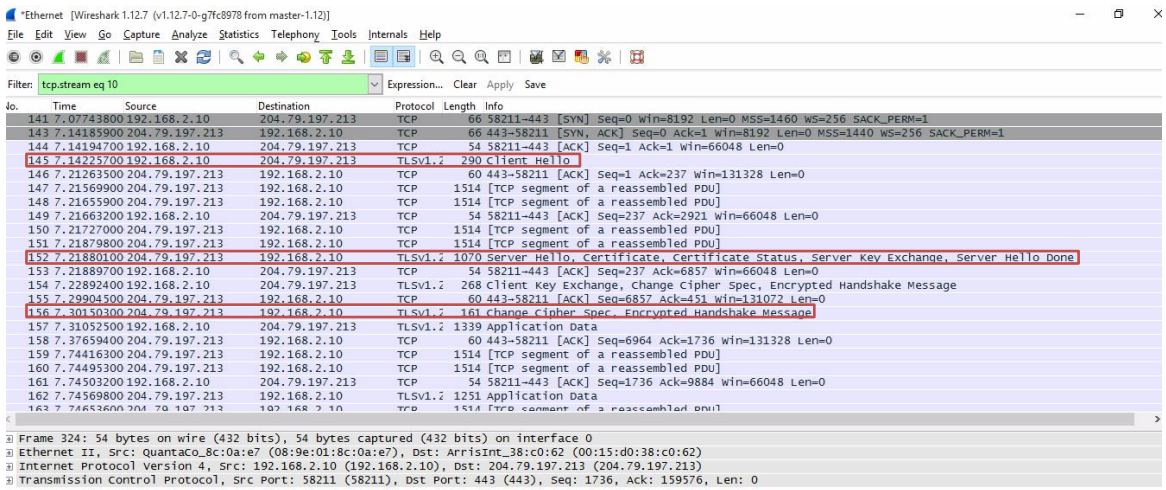
9) Cerficate Verify: El cliente le dice al servidor tengo las claves, empecemos la transferencia de datos.

10) Finished: se termina la negociación y empieza la transferencia de datos.

Las Figura 1 muestra un diagrama temporal de los mensajes recién citados intercambiados entre servidor y cliente.

6. Captura de paquetes de OneDrive en Wireshark:

Se subió a una cuenta de OneDrive el archivo Alice.txt y capturamos diferentes paquetes (TCP y TLSv1.2), donde nos dimos cuenta de los mensajes de negociación del protocolo TLS.



7. Conclusión

Como conclusión por todas la características mencionadas en este informe, nosotros pensamos que OneDrive es la mejor opción a la hora de elegir una nube virtual para almacenar los datos (mayor capacidad de almacenamiento, económico, seguridad de dos pasos, etc). Eso sí, queda al criterio de cada persona, ya sea por sus gustos, dinero, entre otros, elegir la nube virtual que desea utilizar, ya que nuestro enfoqué va hacía la seguridad que brinda OneDrive, con su protocolo TLS. A pesar que ha habido noticias de agentes maliciosos desencriptado archivos de estas nubes (con los protocolos antiguos), sigue siendo un buen medio de almacenamiento de datos. Eso sí, se recomienda tener cuidado con los archivos que se suben a la red.

8. Anexos:

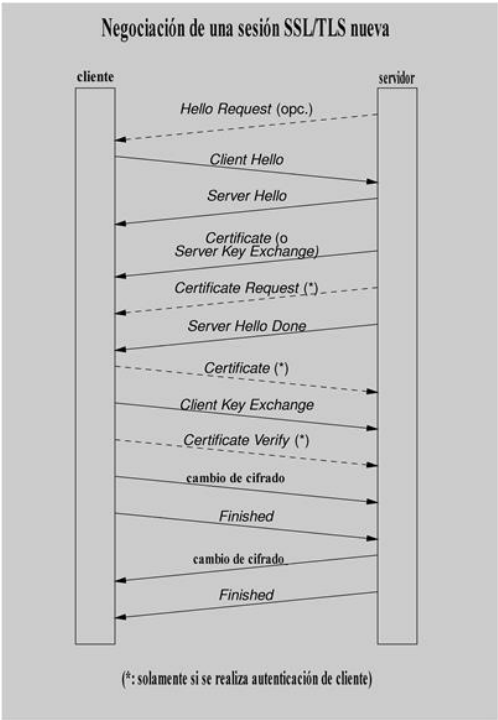


Figura 1

9. Referencias:

[1] https://es.wikipedia.org/wiki/OneDrive

[2] http://www.eldiario.es/turing/moviles_y_tabletas/Consejos-mantener-fotos-seguras- nube_0_298870961.html

[3] https://news.microsoft.com/es-xl/avanzamos-en-nuestros-esfuerzos-de-cifrado-y-transparencia/

[4] http://deic.uab.es/material/26118-ssl.pdf