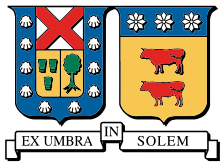


Redes de Computadores I

Proyecto

Dropbox

Guillermo Castro
201021015-4

Javier Garcés
201021002-2

4 de septiembre de 2013

1. Resumen

La sincronización de archivos es hoy, y cada vez más, un elemento importante en cualquier ambiente de trabajo, y son muchas las alternativas de servicios que ofrecen soluciones. Dentro de estos servicios se encuentra Dropbox, que utiliza computación en la nube para llevar a cabo la sincronización. En este trabajo se analiza Dropbox utilizando la herramienta de análisis de paquetes Wireshark.

Para cumplir lo anterior se crearon tres escenarios que abarcan las situaciones de trabajo de este servicio, estas son: respaldo de archivos locales en la nube, sincronización de archivos a través de internet , y sincronización de archivos en una red local.

Luego del análisis vía Wireshark se puede observar que para respaldo de archivos, estos se suben directamente a una de las direcciones IP de Dropbox, similarmente en sincronización de archivos, el cliente que sube el archivo lo hace directamente a Dropbox y luego Dropbox contacta a los clientes que también requieran el archivo. Para el caso de sincronización en LAN, los archivos entre clientes se comparten directamente entre ellos. Para todos los casos las transferencias realizan por TLS.

2. Introducción a Dropbox

2.1. Historia de Dropbox

Dropbox nace a partir de una idea de Drew Houston, un estudiante del MIT que cansado de extraviar sus dispositivos de almacenamiento, imagina un servicio que utilizara la computación en la nube para solucionar el problema de la sincronización de archivos. Para impulsar su idea acude a `YCombinator.com`, un sitio de crowd-funding, con lo que consigue los fondos suficientes para impulsar su idea y lanzar oficialmente Dropbox en 2008 [3]. Hoy en día es un servicio utilizado por más de 100 millones de personas en el mundo [1] siendo responsable del 0.29 % del ancho de banda mundial [2].

2.2. Análisis de paquetes

El impacto generado por este servicio sumado a lo cotidiano de su uso en un ambiente de trabajo como el universitario, además de la necesidad de conocer que tipo de seguridad posee Dropbox, motivan el estudio de funcionamiento de Dropbox aprovechando que mediante Wireshark se puede transparentar, a través de la lectura de paquetes, la manera en que Dropbox funciona, tanto en la nube como el LAN.

3. Protocolos DB-LSP y DB-LSP-DISC

Para la sincronización en red local Dropbox utiliza dos protocolos propietarios de manera que se pueda utilizar la red local en vez de internet para transferir archivos entre clientes ,cuando sea posible, y así optimizar el tiempo que toma el proceso de sincronización. Estos protocolos son `Dropbox LAN Sync Protocol` y `Dropbox LAN Sync Discovery Protocol`. A continuación se detallan estos protocolos.

3.1. DB-LSP-DISC

Dropbox LAN Sync Discovery Protocol se encarga de buscar clientes de Dropbox disponibles en la red local para transferir archivos. Consiste en paquetes UDP enviados a la dirección de broadcast de la red. Los clientes responden a la dirección del computador emisor en el puerto 17500. Estos mensajes son enviados periódicamente a la red cada 20∼30 [s] [4].

193	23.307435000	192.168.1.234	255.255.255.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol
194	23.308605000	192.168.1.234	255.255.255.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol
195	23.308681000	192.168.1.234	192.168.1.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol
524	49.361929000	192.168.1.234	255.255.255.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol
525	49.363022000	192.168.1.234	255.255.255.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol
526	49.363082000	192.168.1.234	192.168.1.255	DB-LSP-	285 Dropbox LAN sync Discovery Protocol

Figura 1: Captura de los paquetes DP-LSP-DISC, se puede apreciar el envío a las direcciones de broadcast y el intervalo temporal de envío, que en este caso corresponde a 26 [s].

3.2. DB-LSP

Los mensajes DB-LSP son encargados de enviar mensajes de control entre clientes cuando se realizan transferencias de archivos. Estos mensajes utilizan el protocolo TCP y son enviados también al puerto 17500 de cada cliente participante en la transferencia [4].

1620	17.771132000	192.168.1.182	192.168.1.234	DB-LSP	452 Dropbox LAN sync Protocol

Figura 2: Ejemplo de paquete DB-LSP enviado durante la tranferencia de un archivo, notar que ambas IP's corresponden a una red local.

4. Respaldo de Archivos Locales

La principal función del servicio Dropbox es de almacenamiento en la nube. Al crear una cuenta Dropbox, un usuario tiene 2 GB de almacenamiento disponibles en los servidores de Dropbox, lo que permite mantener archivos propios en servidores externos, con la ventaja de poder usar el espacio como respaldo o para almacenamiento sin necesidad de usar capacidad del disco duro propio.

Al crear una cuenta, se ofrece al usuario descargar la aplicación, cuya función es identificar actualizaciones en las carpetas asociadas a Dropbox e iniciar la conexión con el servidor.

El procedimiento de respaldo de un archivo se puede analizar capturando los paquetes enviados y recibidos usando el software *Wireshark*. Este proceso sigue una secuencia de pasos cada vez que se añade un nuevo archivo a la carpeta asociada a Dropbox:

1. Se hace una consulta DNS para encontrar la dirección IP destino de la base de datos de Dropbox para almacenar el archivo.

46	3.344572000	192.168.1.182	192.168.1.1	DNS	81 Standard query 0x45f1 A client-lb.
47	3.346344000	192.168.1.1	192.168.1.182	DNS	320 Standard query response 0x45f1 CNA

Figura 3: Paquetes DNS, Usuario transmisor

2. Se realiza el establecimiento de conexión, mediante paquetes indicados en *Wireshark* como *Client Hello* y *Server Hello*.

53	3.534759000	192.168.1.182	199.47.216.172	TLSv1	128 Client Hello
54	3.718597000	199.47.216.172	192.168.1.182	TCP	60 https > 49596 [ACK] Seq=1 Ack=75 W
55	3.725546000	199.47.216.172	192.168.1.182	TLSv1	1434 Server Hello

Figura 4: Paquetes de establecimiento de conexión, Usuario transmisor

3. Se prosigue al envío del archivo, particionado en varios paquetes. Esta información es encriptada según el protocolo de seguridad TLSv1 y se emplea TCP para un envío seguro y sin pérdidas del archivo a la base de datos de Dropbox.

301	6.163751000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
302	6.163787000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
303	6.163821000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
304	6.163854000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
305	6.163891000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
306	6.163927000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data
307	6.163963000	192.168.1.182	23.23.127.94	TLSv1	1434 Application Data

Figura 5: Paquetes de archivo a respaldar, Usuario transmisor

4. Se finaliza la conexión.

2619	34.308003000	199.47.216.172	192.168.1.182	TCP	60 https > 49596 [FIN, ACK] Seq=6151
2620	34.308192000	192.168.1.182	199.47.216.172	TCP	54 49596 > https [ACK] Seq=2303 Ack=

Figura 6: Paquetes de finalización de conexión, Usuario transmisor

5. Sincronización de Archivos

La segunda función importante que debe cumplir el servicio Dropbox es la sincronización de archivos entre varios usuarios. Esto permite la actualización de documentos entre varios miembros de un grupo establecido, y es de gran utilidad en numerosos contextos, como un grupo familiar o de trabajo.

El servicio debe cumplir con ser seguro, tanto en actualizar los archivos compartidos de forma rápida y confiable como en usar encriptación en el envío de paquetes de forma que no sean accesibles por terceros.

Se ha analizado mediante el software *Wireshark* los paquetes enviados a través de la red durante el proceso de sincronización de archivos entre usuarios, quienes no se encuentran en una red local (este caso se detalla en la sección 6). Para ello, un usuario transmisor añade un archivo pequeño en la carpeta compartida y se capturan los paquetes enviados y recibidos por ambos usuarios hasta que el archivo aparece integramente en la carpeta compartida del usuario receptor.

Primero, se realiza el respaldo del archivo añadido por el usuario transmisor, siguiendo el procedimiento descrito en la sección 4.

Luego de finalizado el proceso de respaldo, el usuario receptor es notificado del cambio realizado en la carpeta compartida y sigue una serie de pasos para obtener el archivo sincronizado.

1. Recibe la notificación de actualización mediante un mensaje HTTP, desde Dropbox.

60	45.490904000	108.160.162.43	10.9.12.33	HTTP	255 HTTP/1.1 200 OK (text/plain)

Figura 7: Paquete de inicio de sincronización, Usuario receptor

2. Se prosigue siguiendo los mismos pasos del transmisor: Solicitud DNS, inicio de conexión y transmisión de datos encriptados.

109	47.969071000	10.9.12.33	23.23.107.43	TLSv1	480 Application Data, Application Data
110	48.181653000	23.23.107.43	10.9.12.33	TCP	60 https > 49514 [ACK] Seq=4067 Ack=699 Win=168
111	48.898856000	23.23.107.43	10.9.12.33	TCP	1434 [TCP segment of a reassembled PDU]
112	48.899496000	23.23.107.43	10.9.12.33	TCP	1434 [TCP segment of a reassembled PDU]
113	48.899524000	10.9.12.33	23.23.107.43	TCP	54 49514 > https [ACK] Seq=699 Ack=6827 Win=165
114	48.900046000	23.23.107.43	10.9.12.33	TCP	1434 [TCP segment of a reassembled PDU]
115	48.901113000	23.23.107.43	10.9.12.33	TCP	1434 [TCP segment of a reassembled PDU]

Figura 8: Paquetes de datos de archivo encriptados, Usuario receptor

Cabe destacar que, en la figura 8, la dirección IP del usuario receptor es 10.9.12.33 y recibe los segmentos del archivo desde la dirección IP 23.23.107.43. Un análisis en un servicio identificador de IP permite conocer

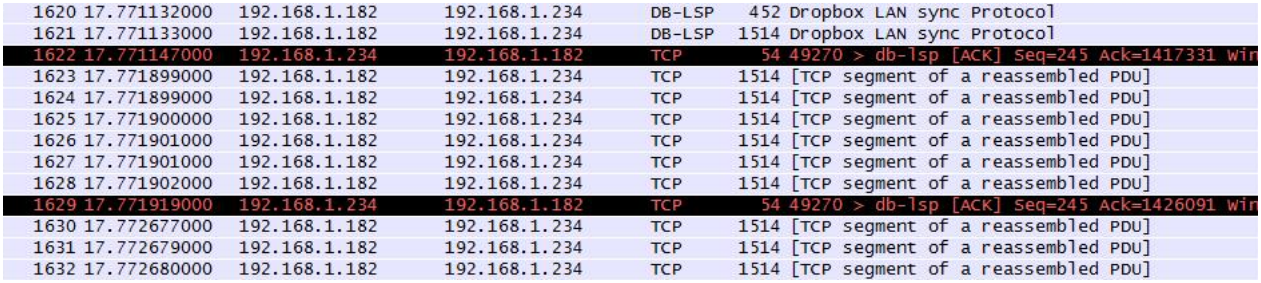
que esta última dirección está asociada a la empresa Amazon. Esto se debe a que Amazon es propietario de los servidores que Dropbox usa para almacenar estos archivos.

6. Sincronización de Archivos en Red Local

En el caso de sincronización entre usuarios en la misma red, el proceso es diferente para el usuario receptor.

El usuario transmisor sigue los mismos pasos descritos en la sección 4. El usuario receptor, por su lado, ya ha identificado la presencia del usuario en su red local, mediante el protocolo DB-LSP-DISC descrito en la sección 3.

Entonces, el usuario receptor, en vez de descargar el nuevo archivo desde la base de datos de Dropbox, la descarga directamente desde el computador del usuario en la red local. Esto es conveniente en términos de congestión y velocidad de transmisión.



1620	17.771132000	192.168.1.182	192.168.1.234	DB-LSP	452	Dropbox LAN sync Protocol
1621	17.771133000	192.168.1.182	192.168.1.234	DB-LSP	1514	Dropbox LAN sync Protocol
1622	17.771147000	192.168.1.234	192.168.1.182	TCP	54	49270 > db-lsp [ACK] Seq=245 Ack=1417331 Wir
1623	17.771899000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1624	17.771899000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1625	17.771900000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1626	17.771901000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1627	17.771901000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1628	17.771902000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1629	17.771919000	192.168.1.234	192.168.1.182	TCP	54	49270 > db-lsp [ACK] Seq=245 Ack=1426091 Wir
1630	17.772677000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1631	17.772679000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]
1632	17.772680000	192.168.1.182	192.168.1.234	TCP	1514	[TCP segment of a reassembled PDU]

Figura 9: Paquetes de datos de archivo encriptados, Usuario receptor, Sincronización en red local

Se observa el uso del protocolo DB-LSP durante el proceso de sincronización LAN, que corresponde al protocolo anteriormente descrito en la sección 3.2.

7. Conclusiones

El propósito de Dropbox es dar solución a la necesidad de respaldo de archivos (almacenamiento en la nube) y de sincronización entre usuarios.

La solución que implementa el servicio es un sistema organizado de almacenamiento en servidores externos y de control de sincronización entre usuarios, mediante software para computadores personales y procedimientos de intercambio de paquetes. Además, se brinda un servicio que cumple con seguridad de información (encriptación) y transmisión confiable de archivos.

Ha sido posible analizar el funcionamiento del servicio mediante el software *Wireshark*, observando el intercambio de información entre usuario y servidor. Así, se han identificado los protocolos propietarios de Dropbox y los distintos procedimientos que son llevados a cabo para cumplir con el servicio ofrecido.

Actualmente, existen numerosos servicios que compiten directamente con Dropbox al ofrecer variaciones del mismo servicio. Esto permite comprender la gran necesidad para los usuarios, tanto en un ámbito personal como grupal, de respaldo y sincronización.

Referencias

[1] *The Dropbox Blog*, blog.dropbox.com.

[2] Paloalto Networks, *Application usage and threat report*, researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization/.

[3] Wikipedia English, *Dropbox*, en.wikipedia.org/wiki/Dropbox_(service).

[4] Geeklogsblog, *Dropbox: LAN sync protocol*, geeklogsblog.wordpress.com/2011/09/10/dropbox-lan-sync-protocol/