>> Jorge Dávila

La Internet opaca de SPDY

La hegemonía de los terminales móviles está causando cambios en lo que conocemos como Internet. Las limitaciones en los anchos de banda exigen una mayor eficiencia en el protocolo de comunicación y para atender esa demanda aparece SPDY, un nuevo protocolo que lleva asociado el cifrado de todas las comunicaciones web. Esta novedad volvería opacas las arterias por las que hoy fluyen los datos de Internet y eso tendrá consecuencias para la defensa de los derechos ciudadanos, colectivos e individuales, y por ello es conveniente prestarle algo de atención.

Cuando Tim Berners-Lee y su equipo diseñaron el protocolo de aplicación HTTP[1] en el mes de marzo de 1989[2], no pensaron que las páginas que habría de transportar llegasen a ser tan complicadas como las actuales. Dicha invención fue acompañada de la definición de información "hipermedia"[3] y esa es la base sobre la que se asienta lo que conocemos como World Wide Web. Por debajo de HTTP está el protocolo de conexión y transferencia ordenada de datos conocido como TCP[4], y debajo de él está el protocolo IP, que se encarga de la comunicación mediante el uso de paquetes de información.

HTTP funciona como un protocolo de solicitud-respuesta dentro del modelo computacional de cliente-servidor. El cliente envía un mensaje HTTP de solicitud al servidor y este, que dispone de la información solicitada (fichero HTML o de otro tipo) o hace las funciones pedidas por el cliente, le devuelve un mensaje de respuesta.

Cuando nació Internet no se podía imaginar que la guerra de los terminales fuese a terminar siendo ganada por los terminales móviles que llamamos *smartphones*[6], y que estos iban a introducir los límites que lo marcarían todo: el ancho de banda disponible, la capacidad electroquímica de las baterías de más alta tecnología y, por último, el peso de todo ese artefacto. En realidad, el factor limitante no está en el hardware. Para navegar no sirve de mucho utilizar procesadores más potentes, que calentarían el terminal y consumirían más potencia. El límite actual realmente está en la red inalámbrica (3G, LTE, 4G, etc.) de la que todos terminamos colgados.

La comunidad internacional está dispuesta a corregir aquellos enfoques simplistas de entonces. La idea es acelerar el tiempo de descarga de las páginas web en dispositivos móviles. Para ello, lo primero que se hace es reunir en una misma conexión la descarga de todos los elementos que componen dicha página web. Actualmente, en el protocolo HTTP, se hace una conexión TCP distinta para descargar cada elemento, incluso para traer el más humilde GIF que represente un botón o una leve sombra en esas sofisticadas páginas que algunas estéticas dictan.

Además de reunir en una todas las conexiones relacionadas entre sí, también se utiliza una posibilidad que siempre ha estado ahí pero que, con el crecimiento de la velocidad de las redes de comunicación siguiendo la Ley de Moore y la obsesión por ahorrarse ciclos de computación en los servidores, nunca fue vista como una necesidad y no se utiliza. Nos referimos a la posibilidad de que el servidor comprima los datos antes de enviarlos y que el cliente proceda a descomprimirlos cuando los reciba.

Un sistema de comunicaciones a prueba de intercepciones dificultaría mucho la acción de la ley sobre los que utilizan el ciberespacio. Las investigaciones policiales, las pruebas judiciales o incluso el propio espionaje, tendrán que volver a tecnologías, usos y costumbres propios de la era pre-Internet; más aún, el regreso sería a los tiempos en los que no había comunicaciones a distancia, ya que todas las comunicaciones se harán a través de esa red opaca y no habrá teléfonos que pinchar o sobres que cuidadosamente abrir.

Pasarela SPDY-HTTP

SPDY[8] es un protocolo abierto de red desarrollado principalmente por Google para el transporte de contenidos web. Esta nueva versión manipula el tráfico HTTP para reducir la latencia de carga de las páginas web utilizando la compresión, el multiplexado y la priorización de paquetes. Además de eso, el nuevo protocolo incluye una significativa mejora en la seguridad de esa comunicación. En julio de 2012, los desarrolladores de SPDY manifestaron que estaban trabajando en su estandarización, de modo que el primer borrador del futuro protocolo HTTP 2.0 utilizaría SPDY como base para las comunicaciones en red. Actualmente, las implementaciones de SPDY en los navegadores son mucho más comunes de lo que cabría pensar; de hecho, las encontramos en las últimas versiones de los navegadores Chromium[9], Firefox, Opera, Amazon Silk e Internet Explorer.

En SPDY el uso del protocolo de cifrado TLS[10] es obligatorio, y las cabeceras de

[1] Ver **Hypertext Transfer Protocol** en http://en.wikipedia.org/wiki/Http (RFC 2616 y 2617)

[2] Ver http://en.wikipedia.org/wiki/History_of_the_World_Wide_Web

[3] Ver http://en.wikipedia.org/wiki/Html

[4] TCP = Transmission Control Protocol. Ver http://en.wikipedia.org/wiki/Transmission_Control_Protocol

[5] IP = Intenetprotocol. Ver http://en.wikipedia.org/wiki/Internet_protocol

[6] En el número de mayo de 1970 de la revista Popular Science, Arthur C. Clarke predijo que los satélites algún día "*bring the accumulated knowledge of the world to your fingertips using a console that would combine the functionality of the photocopier, telephone, television and a small computer, allowing data transfer and video conferencing around the globe*". Sólo se equivocó en lo de los satélites y no imaginó las redes de fibra óptica.

[7] Ver http://en.wikipedia.org/wiki/List_of_energy_densities#Common_energy_densities

[8] "SPDY" es una marca de Google y no es ningún acrónimo. Draft IETF http://tools.ietf.org/id/draft-mbelshe-httpbis-spdy-00.txt. También ver http://dev.chromium.org/spdy/spdy-whitepaper.

[9] Ver http://www.chromium.org/Home

[10] Ver http://en.wikipedia.org/wiki/Transport_Layer_Security

transmisión son comprimidas, por diseño, con el algoritmo DEFLATE[11], mientras que en la versión actual de HTTP, esas cabeceras van en claro y son humanamente legibles. En este nuevo protocolo, los mensajes intercambiados son pre-procesados, asociados con tokens, simplificados y comprimidos. Por ejemplo, en cada nodo SPDY se guarda una lista con referencias a las cabeceras de los objetos que ya se han enviado dentro de esa sesión, lo que permite evitar el re-envío de algo que ya se tiene y no ha cambiado.

Otra característica interesante es que, en este nuevo protocolo, el servidor no tiene por qué esperar a que el cliente le solicite las cosas, él **puede entregar** (*push*) **contenido no solicitado al cliente**, lo cual puede terminar siendo, entre otras cosas, un desperdicio de ancho de banda. SPDY requiere el uso de SSL/TLS con la extensión NPN[12], y **no acepta trabajar con el HTTP que hoy conocemos**.

SPDY no reemplaza a HTTP, sino que modifica esencialmente el modo en el que se envían las peticiones y respuestas a través de la línea de comunicación. Por ello, todas las aplicaciones actuales de servidor sólo pueden utilizarse sin modificación alguna si delante de ellas se coloca un traductor, una pasarela SPDY-HTTP.

Transición

Un cambio tan importante no puede hacerse de la noche a la mañana por lo que es razonable pensar en un largo periodo de transición en el que sólo una pequeña cantidad de los servidores que componen Internet trabajen con el nuevo protocolo. En el mes de abril de 2013, aproximadamente un 1% de todos los servidores web hablaban SPDY. Desde entonces, ha habido un descenso de esa población hasta el 0,6%. Sin embargo, desde enero de este año[13] algunos servicios de Google (Google search, Gmail y otros que utilizan SSL) utilizan SPDY, siempre que esté disponible en el navegador del usuario. Otros sitios web que también utilizan el protocolo son: Google [.com.co.in.de.fr.co.uk], Facebook, Youtube, Twitter, Wordpress y Tumblr.

Para favorecer la adopción de ese nuevo paradigma, o para satisfacer otros intereses menos altruistas, Google puso en funcionamiento "*gateways*" que se encargan de traducir ambos protocolos e invitó a usuarios de terminales móviles a probarlos. Con el uso de esas pasarelas de Google, las comunicaciones entre ellas y el terminal móvil del usuario son (1) más eficientes (descarga más rápida), en ellas (2) **Google lo sabrá todo sobre nuestros hábitos de navegación, lo cual se suma al conocimiento de nuestras inquietudes a través de las preguntas que le hacemos**, y (3) la comunicación estará completamente cifrada, de modo que todo el que no sea el terminal móvil o la pasarela de Google, estará ciego respecto a lo que se está comunicando.

Que Google haya sido el primero en montar una infraestructura para poner a prueba el nuevo protocolo, no significa que no puedan ser otros, otras iniciativas, otros intereses, los que monten constelaciones de esas pasarelas y se conviertan, **probablemente sin saberlo el usuario**, en su "*ciberconfesor*" para el que ningún detalle de su navegación le será ajeno.

Intimidad y oscuridad

Una pregunta difícil de contestar es la de cuánto duraría esa transición. Si nos fijamos en otros cambios de estándar y la querencia comercial que hay a la compatibilidad hacia atrás, muy probablemente estemos hablando de más de una década. Durante ese tiempo, las pasarelas serán las que controlen y conozcan realmente a sus usuarios, y los que no gestionen esas pasarelas tan sólo verán secuencias binarias sin sentido.

En el futuro, cuando se dé por terminada la transición HTTP 1.1 → 2.0, cada navegador se conectará con cualquier servidor utilizando el protocolo SPDY, que para entonces habrá evolucionado, y las comunicaciones, además de ser más eficientes, también serán privadas y lo que se comunique será asunto de los interlocutores y, en principio, de nadie más. Según esto, **el riesgo para la intimidad de los usuarios está en el periodo de transición y no en el destino final**.

Por otra parte y de forma independiente a la iniciativa SPDY, todavía sigue abierto el frente de una "Internet de dos velocidades"[14] en las que los operadores de redes sueñan con encontrar los réditos que no consiguen por ser meros transportadores de señal y no generadores de valor. El flamante éxito comercial de negocios como Google o Facebook despierta la envidia de los propietarios de las redes que los hacen posibles. Para corregir esa subjetiva "injusticia", algunos poderes proponen o reclaman vehementemente que el medio cibernético no sea igual para todos.

Esa Internet de dos velocidades consiste sencillamente en la segregación entre los que pueden pagar y pagan, y todos los demás. Para los primeros podrá haber redes telemáticas veloces, llenas de valor añadido, eficientes e incluso discretas; sin embargo, para los demás, la calidad será sustancialmente inferior.

Aunque oficialmente nada de eso ocurre todavía, hay quejas de instituciones como la BBC, respecto a que hay ISPs que, de forma reiterada y deliberada, disminuyen selectivamente las velocidades de transmisión muy por debajo de los valores publicados y que transportan ciertos contenidos más deprisa que otros[15].

Una de las ventajas de cualesquiera soluciones que como SPDY popularicen el

SPDY no reemplaza a HTTP, sino que modifica esencialmente el modo en el que se envían las peticiones y respuestas a través de la línea de comunicación. Para favorecer la adopción de ese nuevo paradigma, Google puso en funcionamiento "gateways" que se encargan de traducir ambos protocolos e invitó a usuarios de terminales móviles a probarlos. Con el uso de esas pasarelas de Google, las comunicaciones entre ellas y el terminal móvil del usuario son más eficientes. Pero Google lo sabrá todo sobre nuestros hábitos de navegación, lo cual se suma al conocimiento de nuestras inquietudes a través de las preguntas que le hacemos. Y la comunicación estará completamente cifrada, de modo que todo el que no sea el terminal móvil o la pasarela de Google, estará ciego respecto a lo que se está comunicando.

[11] Ver http://en.wikipedia.org/wiki/DEFLATE

[12] NPN = Next Protocol Negotiation. Ver http://en.wikipedia.org/wiki/Next_Protocol_Negotiation

[13] Ver http://w3techs.com/technologies/details/ce-spdy/all/all

[14] Ver http://www.nytimes.com/2014/04/25/opinion/creating-a-two-speed-internet.html

[15] Ver http://www.theguardian.com/media/2011/jan/19/mark-thompson-internet-bbc

cifrado extremo-a-extremo es que el papel de las operadoras volverá a limitarse y centrarse en mantener la calidad de servicio independientemente del contenido o naturaleza de éste.

Con la adopción y universalización de las comunicaciones cifradas, no solo las empresas operadoras de las redes de telecomunicación se quedarán ciegas, también sufrirán ese mal las universidades, la administración pública, las empresas, los hogares, todo el mundo. Si los navegadores utilizados y los servidores de Internet hablan SPDY, el contenido de sus conexiones quedará fuera del alcance de *firewalls*, detectores de intrusión, analizadores de *malware*, "*Deep Packet Inspectors*" [16], etc. Gracias al cifrado, el destino de las grandes operadoras de telecomunicaciones será también el de cada uno de los CPDs que cooperativamente componen Internet: la oscuridad.

La adopción generalizada de cualquier protocolo con cifrado robusto no sólo supone cegar a los operadores de red, sino también a las fuerzas de seguridad del estado y a las agencias de inteligencia, que entrarán en el reino de la oscuridad telemática, lo cual es una amenaza clara para sus funciones y habrán de encontrar el modo de responder a ello.

En un ciberespacio en el que todas las comunicaciones estén cifradas, desaparecen las muchas facilidades que la actual tecnología Internet ha proporcionado durante décadas a jueces, policías y responsables de la seguridad nacional para el conocimiento de las actividades de ciudadanos, grupos organizados de todo tipo y empresas. En principio, **el uso del cifrado confinará la comunicación a los terminales de los contertulios y aportará una intimidad que actualmente no existe en Internet**.

Un sistema de comunicaciones a prueba de intercepciones dificultaría mucho la acción de la ley sobre los que utilizan el ciberespacio. Las investigaciones policiales, las pruebas judiciales o incluso el propio espionaje, tendrán que volver a tecnologías, usos y costumbres propios de la era pre-Internet; más aún, el regreso sería a los tiempos en los que no había comunicaciones a distancia, ya que todas las comunicaciones se harán a través de esa red opaca y no habrá teléfonos que pinchar o sobres que cuidadosamente abrir.

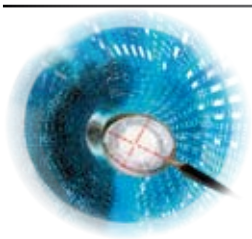
En principio, en una sociedad que utilice una Internet opaca (cifrada) todos los agentes son igualmente ciegos. Sin embargo, las operadoras y con ellas otros, podrán seguir haciendo **Análisis de Tráfico** [17] en vista a deducir informaciones parciales de los comunicantes a través de los patrones de comunicación que puedan ser identificados. De hecho, eso es lo que ya se consigue con los denominados "*metadatos*" de la recientemente anulada [18] Directiva Europea de Conservación de Datos [19].

Independientemente de estas restricciones técnicas, hay que tener en cuenta que **lo que hace más inseguro a un ciudadano, a una empresa, o a una administración es estar convencido de que no necesita protegerse**. Aunque Internet fuese opaca en lo que a las comunicaciones se refiere, el mero hecho de que existan las redes sociales en las que algunos lo cuentan todo, da un respiro y oportunidad a los que quieran o necesiten "investigar" y desvelar secretos personales, comerciales o nacionales. El cifrado de las comunicaciones (si se hace bien) sólo anula un medio, un canal de acceso, un lugar donde se puede escuchar sin ser detectado, pero no es el único escenario [20] en el que se pueden desarrollar las actividades habituales para la obtención de "inteligencia".

Si el problema es no poder descifrar lo que se transmite, el atacante siempre puede coger la información justo antes de que sea cifrada, o cuando acabe de ser descifrada por los que sí pueden hacerlo. En este nuevo escenario las ventanas de ataque se desplazan a los terminales, a los equipos, y eso no es nada nuevo, ya lo hacen desde hace tiempo los caballos de Troya, familiarmente conocidos como "*troyanos*" [21].

Lo que quizás sea más peligroso para el ciudadano y para la sociedad en la que vive es el periodo de transición en el que Internet pueda ser opaca para las fuerzas de seguridad de la inmensa mayoría de los estados soberanos y que, sin embargo, el ciudadano este sometido al más exhaustivo escrutinio por parte del que le presta la constelación de "*pasarelas*" que conectan los universos HTTP 1.1 y SPDY. En ese escenario, **la soberanía real de esos estados quedaría mermada en la misma medida en que sus capacidades de investigación disminuyen** y, sin embargo, las empresas de esas pasarelas lo podrían investigar todo para luego "*paquetizar*" esa información y entregársela al mejor postor, o al más fuerte.

Huelga decir que a ese postor, a esa entidad no la habrá elegido ningún censo amplio de ciudadanos libres e informados siguiendo procedimientos democráticos, ni perseguirá el bien común y universal. ■



Con la adopción y universalización de las comunicaciones cifradas, no solo las operadoras de las redes de telecomunicación se quedarán ciegas, sino que también sufrirán ese mal las universidades, la administración pública, las empresas, los hogares, todo el mundo. Si los navegadores utilizados y los servidores de Internet hablan SPDY, el contenido de sus conexiones quedará fuera del alcance de cortafuegos, detectores de intrusión, analizadores de malware, "Deep Packet Inspectors"... Gracias al cifrado, el destino de las grandes operadoras de telecomunicaciones será también el de cada uno de los CPDs que cooperativamente componen Internet: la oscuridad.

[16] Ver http://en.wikipedia.org/wiki/Deep_Packet_Inspection

[17] Ver http://en.wikipedia.org/wiki/Traffic_analysis

[18] Ver http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

[19] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE

[20] Ver http://en.wikipedia.org/wiki/Social_engineering_(security)

[21] Ver http://es.wikipedia.org/wiki/Troyano_(informática)

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es