Informe sobre IETF 109

Reunión virtual

16 al 20 de noviembre de 2020

El informe fue producido por CENTR y traducido por LACTLD

Agradecemos a Hugo Salgado (NIC Chile) por la revisión de la edición en español

Para acceder a la versión en inglés de este informe, visitar https://centr.org/library

lactld

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Contenidos

I. Introducción

La última reunión del Grupo de Trabajo de Ingeniería de Internet (IETF) de este año fue llevada a cabo nuevamente de forma virtual, lo que convirtió al 2020 en el primer año en que el organismo de normalización organizó reuniones únicamente en línea. Con el Centro de Operaciones de Red del IETF aún intentando encontrar su lugar en reuniones de esta escala, se esperaban inconvenientes técnicos, aunque no arrebataron mucho de la agenda completa de los grupos de trabajo e investigación, que recibieron la participación de un total de más de mil personas.

II. Adaptándonos a la realidad del despliegue del DNS cifrado

¿Qué tienen en común los informáticos, los economistas del comportamiento y los psicólogos cognitivos? Todos valoran el poder del efecto predeterminado; es decir, lo que las personas reciban sin tomar una decisión activa será probablemente lo más popular. En el mundo del desarrollo de protocolos de red, puede decirse que la historia del despliegue de protocolos de DNS cifrado está centrada en torno a lo que se convertirá en el valor predeterminado.

Aunque el DNS tradicional de texto claro sigue siendo el más común, el futuro de la opción por defecto del DNS cifrado aún está al alcance de cualquiera. Actualmente, el grupo de trabajo de Adaptive DNS Discovery (WG de ADD) cuenta con varias propuestas de proveedores de servicios de Internet, proveedores de servicios en la nube y navegadores web.

Contexto

El Sistema de Nombres de Dominio (DNS) es la manera en que los nombres que podemos leer los humanos (como centr.org) se traducen a sus respectivas direcciones de red (por ejemplo, 178.208.52.35 o 2a00:1 c98:10:60:ffff:ffff:ffff:10) para que podamos conectarnos a ellas. Principalmente, estas consultas se han llevado a cabo, por lo general, en texto plano y, por ende, han carecido de garantías de seguridad y privacidad. Los proveedores de servicios de Internet, que tradicionalmente ofrecieron estos servicios a los usuarios, pueden ver qué sitios visita el usuario. Los atacantes en tránsito también podrían ver fácilmente dicha información e incluso podrían bloquear ciertos sitios web en función a ella.

La posibilidad de contar con más privacidad en estas consultas apareció finalmente con la estandarización de protocolos como DNS sobre TLS (DoT) y DNS sobre HTTPs (DoH) en 2016 y 2018, respectivamente. Si bien hubo consenso en que estos protocolos aumentan la privacidad en tránsito, aún persiste una inquietud: ¿quién puede ver, finalmente, estas consultas? Los proveedores de servicio de Internet (ISP) se preocuparon por el hecho de que las aplicaciones pudieran fácilmente hacer consultas DoH a cualquier resolutor que quisieran,

evitando los ISP por completo. Esta información privada ahora estaría disponible para empresas tecnológicas importantes que operan los navegadores o servicios en la nube, que han estado involucradas en el desarrollo o el despliegue del DoH.

La Asociación de Proveedores de Servicios de Internet del Reino Unido nominó a Mozilla como "villano de Internet" por planificar el despliegue del DoH en una manera que evitaba a los proveedores y a sus mecanismos de filtrado de contenidos. La Asociación Europea de Operadores de Redes de Telecomunicaciones publicó un documento de posición en el que expresó sus preocupaciones por el hecho de que todo el tráfico DNS pueda moverse en una pequeña cantidad de actores, y solicitó un mayor escrutinio del impacto del despliegue del DoH en la regulación y la competencia en la industria.

Es posible que los nuevos desarrollos en el IETF tengan importantes consecuencias políticas, dado que los reguladores en la UE y el resto del mundo están cada vez más sensibilizados ante las preocupaciones de privacidad y de derecho de la competencia en la industria tecnológica.

¿Qué está sucediendo ahora?

Si bien Mozilla hizo que el valor predeterminado fuera el DoH para sus usuarios en EE. UU., el fuerte contragolpe a esto atrajo la atención de los reguladores del Reino Unido, haciendo que frenaran sus planes para hacer lo propio en el Reino Unido. Varios desarrollos en el IETF dan una idea de lo que puede pasar si el DoH y el DoT se implementan cada vez más alrededor del mundo.

En lugar de usar directamente resolutores DNS terceros, es posible que existan dos razones para seguir usando los resolutores de los ISP (con DoH/DoT en lugar de DNS de texto plano). En primer lugar, los ISP pueden seguir brindando controles parentales y otros tipos de servicios de filtrado si los clientes así lo prefieren (o si están sujetos a ellos de manera involuntaria). En segundo lugar, las relaciones que tienen los ISP con los proveedores de servicios en la nube locales pueden implicar mejores respuestas; es decir, las direcciones de red que proveen en respuesta a las consultas DNS pueden estar más cerca, por lo que dichas respuestas pueden resultar en un ruteo de tráfico más eficiente.

A principios de este año, se estableció el WG de ADD en el IETF para explorar algunas preguntas relacionadas: ¿cómo puede un usuario o un dispositivo descubrir resolutores DNS que estén disponibles para ellos en sus redes? ¿Cómo puede un usuario seleccionar uno de ellos si existen múltiples resolutores disponibles?

¡Que se añada una opción DHCP!

Tradicionalmente, un dispositivo elige el resolutor DNS que su punto de acceso le indica mediante el protocolo de configuración dinámica de host (DHCP). El punto de acceso recupera estos detalles desde su ISP. Por lo tanto, una manera de

implementar una opción para que su ISP indique a un dispositivo usar su resolutor DoH/DoT es contar con una opción en el DHCP para poder hacerlo, idea que fue propuesta por un grupo de ingenieros en el *draft* llamado *DHCP and Router Advertisement Options for Encrypted DNS Discovery within Home Networks*.

El descubrimiento de resolutores "equivalentes"

En la agenda del WG de ADD durante la reunión IETF109, no obstante, se encontraba el Descubrimiento de Resolutores Cifrados Equivalentes, que tiene un enfoque distinto sobre este asunto. Desarrollada por tecnólogos de Apple, Microsoft, Cloudflare y Fastly, la propuesta busca responder la pregunta específica de qué puede hacer un dispositivo una vez que cuenta con un DNS tradicional en el que, al parecer, confía: ¿cómo puede descubrir un servicio equivalente que use, en cambio, DoH o DoT? En el caso usual, el *draft* propone que cada dispositivo lleve a cabo una consulta DNS adicional (que use el enlace de servicios y registros de parámetros, desarrollados de manera independiente en el IETF) cuando descubra que existe un resolutor no cifrado: la respuesta a esta consulta contendrá información sobre cómo contactar resolutores relacionados que sean compatibles con los protocolos de DNS cifrado.

Por supuesto, sería poco usual por parte de los participantes del IETF desperdiciar una oportunidad de pedantería. La discusión sobre qué podría significar el término "equivalente" duró alrededor de dos horas en la reunión IETF109.

Diferentes salas, diferentes preguntas

Un *draft* tuvo lugar en el contexto de Mozilla, que agregó a su lista de programa de resolutores de confianza a ComCast, un gigante de las telecomunicaciones de EE. UU. Su *draft*, titulado *CNAME Discovery of Local DoH Resolvers*, propone que un nombre 'doh.test' quede reservado para una consulta DNS CNAME para el descubrimiento de resolutores DoH. Una aplicación (como el navegador Firefox de Mozilla) puede llevar a cabo esta consulta con DNS de texto plano tradicional: si recibe una respuesta con un resolutor que existe en el programa de resolutores de confianza, la aplicación usará dicho resolutor en lugar de usar el predeterminado (que, para Firefox, es actualmente Cloudflare en EE. UU.).

Un clima cambiante

Mientras que las primeras conversaciones sobre DoH parecieron indiferentes sobre el rol de los ISP, la fase actual de la discusión se centra en la participación de estos (o al menos en el despliegue con su participación). De todos modos, dos cosas están quedando cada vez más claras. En primer lugar, el DNS cifrado llegó para quedarse. En segundo lugar, con todas las propuestas recibidas en el IETF, puede que el despliegue de DoH/DoT a escala global sea más conservador de lo que se esperaba: al menos en lo inmediato, no ha concentrado el poder en las

manos de los navegadores web. En términos más sencillos, puede que los proveedores de servicios de Internet continúen cumpliendo una función importante en la provisión de servicios DNS para sus usuarios.

III. La estandarización de un protocolo de mensajería cifrado de extremo a extremo en el IETF

El mes pasado, un informe periodístico austríaco armó revuelo sugiriendo que el Consejo de la Unión Europea se encontraba en la elaboración de una resolución para prohibir el uso de comunicaciones cifradas de extremo a extremo. Esta aseveración se rectificó rápidamente: la resolución propuesta, de hecho, confirma la posición previa de los documentos de políticas de la UE que reconocen la importancia del cifrado de extremo a extremo (E2EE) en la provisión de comunicaciones seguras y privadas.

Si bien la Comisión Europea ha estado tomando en consideración inquietudes sobre el E2EE y el acceso a la información por parte de las agencias de aplicación de la ley desde 2016, no han surgido propuestas vinculantes ni serias que amenacen el uso popular de las comunicaciones con E2EE. Un par de acontecimientos, sin embargo, predicen cierto grado de incertidumbre sobre cuánto se mantendrá esta posición en el futuro.

A comienzos de este año, Politico filtró documentos que revelaban debates de un grupo de trabajo de la Comisión Europea sobre las "soluciones técnicas" para detectar contenido de abuso sexual de menores en comunicaciones privadas con E2EE, como las que brindan Signal y WhatsApp. Organizaciones de la sociedad civil temen que estas propuestas, que incluyen escaneo de contenido en el extremo del cliente y "acceso excepcional" a datos cifrados, menoscaben las garantías de seguridad y privacidad que provee la mensajería con E2EE.

La segunda amenaza para las comunicaciones con E2EE proviene de la lucha contra el terrorismo en la UE. Si bien el *draft* más reciente de la propuesta para la regulación de la diseminación de contenido terrorista en línea no aplica a los servicios de mensajería privada, el coordinador de la lucha antiterrorismo de la UE ha estado promoviendo una postura diferente. En mayo de 2020, les escribió a los estados miembros de la UE para fomentar una "puerta delantera" para el cifrado y una mayor intervención estatal en la regulación del cifrado. En octubre, cuando los Cinco Ojos (EE. UU., el Reino Unido, Australia, Canadá y Nueva Zelanda), la India y Japón emitieron una declaración conjunta en la que solicitaban que estén a disposición los contenidos de las comunicaciones en texto claro para las agencias de aplicación de la ley según estas lo soliciten, el coordinador de la lucha antiterrorismo de la UE acogió con satisfacción la propuesta.

Así, la posición de políticas respecto del E2EE a escala de la UE está dividida en múltiples voces o estancada en una pregunta que en realidad no tiene respuesta: cuando el acceso al dispositivo no sea posible, ¿cómo pueden las agencias de la

aplicación de la ley acceder a mensajes cifrados de extremo a extremo sin "romper" los mecanismos de cifrado? Desafortunadamente, puede que tales aspiraciones en cuanto a estas políticas queden en "una larga lista de maneras tortuosas de conseguir lo imposible."

Atinadamente, una de las maneras recomendadas por el coordinador de la lucha antiterrorismo de la UE es monitorear el desarrollo de los estándares. En sus palabras (traducidas):

"Los estados miembros y las instituciones de la UE deberían estar motivados a desafiar de manera colectiva los cambios en el panorama del cifrado en los organismos de normalización internacionales, en particular del Grupo de Trabajo de Ingeniería de Internet (IETF), para asegurarse de participar en el desarrollo de estándares y normas tecnológicas internacionales, que tendrán un impacto en el cifrado y la ciberseguridad en los años venideros".

Entonces, ¿qué está sucediendo en el IETF?

El WG de Messaging Layer Security (MLS) está inmutado ante estos debates de políticas acerca del cifrado de extremo a extremo. Establecido en 2018, este WG cuenta con un objetivo claro para la estandarización de una arquitectura y un protocolo que puedan facilitar la mensajería cifrada de extremo a extremo. MLS contará con varias propiedades de seguridad claves, que incluyen las siguientes:

- *Confidencialidad del mensaje*: los mensajes no podrán ser leídos por nadie, con excepción del emisor y el receptor.
- *Integridad del mensaje*: los mensajes no podrán alterarse ni manipularse.
- *Autenticidad del mensaje*: los receptores contarán con una garantía sobre la identidad del emisor.
- *Secreto hacia adelante*: la amenaza de una clave en un extremo no causará que las comunicaciones previas sean inmediatamente descifrables.
- *Seguridad posamenaza*: la amenaza de una clave en un extremo no causará que todos los futuros mensajes sean revelados; es decir, se podrán recuperar las propiedades de seguridad incluso después de una amenaza.

Todas las propiedades enumeradas anteriormente ya están garantizadas por algunas soluciones existentes, como el protocolo de Signal, una versión del cual también se utiliza en WhatsApp. Lo nuevo de MLS es su filosofía de diseño: comienza con la mensajería en grupo como valor predeterminado, mientras que protocolos anteriores están diseñados para comunicaciones individuales. La intención es que MLS pueda ser mucho más expansible que las soluciones actuales (como Signal, iMessage, WhatsApp, etc.). Este rendimiento óptimo y la naturaleza abierta del estándar probablemente sean incentivos suficientes para que muchas plataformas y servicios adopten MLS como su protocolo de preferencia para el cifrado de mensajes. Es por esto que, además de los

académicos, el WG cuenta con una participación activa por parte de empresas como Google, Mozilla, Facebook, Twitter y Wire.

¿Se federará?

Dado que los protocolos de E2EE tradicionales han sido diseñados teniendo en mente las conversaciones individuales, la lógica de cómo funcionan los "grupos" de chat ha quedado en manos de los servicios y plataformas particulares. Junto con el hecho de que algunas organizaciones pueden deliberadamente no desear federar sus servicios (por razones comerciales o no comerciales), se puede decir que nunca se consiguió una verdadera interoperabilidad a escala pública en la mensajería con E2EE.

MLS tiene el potencial de cambiar esta realidad. Si bien el WG no estableció la federación ni la interoperabilidad como un objetivo explícito, un *draft* elaborado por autores de Google y Wire indica claramente que esto es técnicamente posible con la arquitectura existente de MLS. Si esto se prueba con éxito, es probable que los detalles sobre cómo lograr la federación con MLS se incorporen en la propuesta a principios de 2021.

El ecosistema aún se mueve

Afortunadamente, el WG de MLS se ocupa de la usabilidad tanto como de la seguridad y la privacidad. Gracias a que los participantes del WG han logrado, de manera proactiva, admitir la compatibilidad con múltiples dispositivos por usuario además de los casos de uso de negocios, MLS ofrece la promesa de un protocolo que se puede desplegar ampliamente en todas las aplicaciones que requieren de una función de mensajería.

Como señala el acta constitutiva de MLS, el WG "espera contar con varias implementaciones interoperables, así como también un análisis exhaustivo de la seguridad" antes de la estandarización. Esto se ratificó en la reunión IETF109, donde se debatió el plan para la especificación del protocolo. El *draft* quedará en suspenso hasta que los desarrolladores obtengan experiencia en el despliegue a partir de la versión actual, y los académicos puedan analizar formalmente las propiedades de cifrado.

Con una entrada amplia en la industria y la probabilidad de implementaciones de código abierto que surgirá en un futuro cercano, el estándar abierto de MLS puede convertirse en la red troncal de las comunicaciones privadas en línea.

IV. ¿Es preocupante desde un punto de vista de la privacidad? Búsqueda inversa en los datos de registros

Desde 2018, la entrada en vigencia del Reglamento General de Protección de Datos (GDPR) ha reactivado las preocupaciones de privacidad vinculadas con los datos de registros en la UE. La pregunta de si la naturaleza tradicionalmente pública de los datos de registros entra en conflicto con los requisitos de protección de datos europeos ya había suscitado conversaciones en ICANN. Si las propuestas recientes en el WG de Registration Protocol Extensions (REGEXT) sirven de indicación, los desarrollos regulatorios en la UE continúan brindando contexto o afectando el establecimiento de estándares sobre los datos de registros también en el IETF.

A partir de enero de 2019, el WG de REGEXT adoptó una especificación que describe cómo añadir capacidades de "búsqueda inversa" al Protocolo de Acceso a Datos de Registro (RDAP). Esta característica recibe su nombre de los varios sitios web que utilizan información pública para brindar capacidades de "Reverse Whois"; es decir, permiten que cualquiera averigüe qué nombres de dominio están registrados por una persona en particular (o bajo una dirección de correo electrónico específica).

¿Por qué usar la búsqueda inversa en absoluto?

Mario Loffredo, quien trabaja en Registro.it y es coautor del *draft*, presentó la propuesta en la reunión del WG de REGEXT durante la IETF109. En particular, gran parte de la breve presentación de Loffredo se centró en contexto regulatorio de la UE que puede hablar de un requerimiento de este tipo de capacidad. Entre otras cosas, Loffredo citó las regulaciones propuestas por la Comisión Europea, pruebas electrónicas (acceso transfronterizo a pruebas electrónicas), que buscan establecer principios claros para el acceso de agencias de aplicación de la ley a información que conservan los proveedores de servicios. Este asunto también se debatió en el 63° Taller Legal y Regulatorio de CENTR.

Además de la aseveración en el *draft* que indica cómo la función puede permitir a "registradores que buscan sus propios dominios", la principal motivación para la estandarización de esta función parece ser facilitar el acceso a la información por parte de las agencias de aplicación de la ley.

Cabe mencionar que la presentación también decía que "las autoridades deberían ser capaces de acceder a datos de registros no públicos sin presentar solicitudes por escrito", afirmación que este autor no pudo corroborar ni conciliar con la regulación propuesta por la CE, que habla específicamente de órdenes judiciales para acceder a tal información.

Otra consideración para la estandarización en el IETF, por supuesto, proviene de los valores del organismo de consenso general y código que funciona. Para este último, los WG generalmente prefieren registrar un interés demostrable en el despliegue de la propuesta técnica antes de que se estandarice, en especial si aún no existen múltiples implementaciones en estado natural. Actualmente, el *draft* enumera al registro italiano como el único que ha implementado esta función como prueba de concepto.

El abordaje de las preocupaciones acerca de la privacidad

Según los autores del *draft*, las preocupaciones sobre privacidad que aplican a Reverse Whois están prácticamente ausentes en su propuesta debido a que el RDAP puede permitir la autenticación antes del acceso a los datos. Aun así, la mayor parte del debate del *draft* se centra ahora en cómo lidiar con las consideraciones de privacidad de señalar tal función como estándar. Algunos participantes piensan que los controles técnicos y organizacionales adecuados pueden mitigar por completo los riesgos a la privacidad: cuando los registros implementen la función, deberán tener un control estricto sobre quién puede realizar estas consultas de "búsqueda inversa", y autenticar su identidad cada vez que lo hagan.

El *draft* cuenta con una sección sobre consideraciones de privacidad, pero es breve y, a grandes rasgos, pide a los registros que sigan los procedimientos legales. Alexander Mayrhofer, quien trabaja en el registro de Austria, señaló que el texto era absurdo, considerando que "no es necesario decir, en un documento técnico, que uno 'debe seguir la ley', ya que eso es bastante obvio".

Ulrich Wisser, del registro nacional de dominios de Suecia, agregó: "¿Cómo sabemos que las consideraciones de privacidad del *draft* son buenas consideraciones de privacidad?" Si bien el proceso del IETF exige una sección sobre consideraciones de privacidad para los estándares y protocolos de red, no existe un requisito similar de enumerar los riesgos para la privacidad y la mitigación asociada con ellos. La RFC 6973, *Privacy Considerations for Internet Protocols*, incluye cierta orientación sobre este respecto, pero no queda claro si los autores del *draft* la tuvieron en cuenta.

Sin ningún otro obstáculo evidente para que el *draft* pase a las siguientes etapas, puede que las próximas discusiones sobre la propuesta nos den un indicio sobre cómo el WG del IETF debatirá sobre las preocupaciones de privacidad, ya que una clara e importante motivación del estándar propuesto es el acceso a la información por parte de agencias de aplicación de la ley.

(Aclaración: quien escribe el presente informe ya ha comentado previamente, a título personal, acerca de versiones más antiguas del *draft*).

V. Llaves y números: ¿el DNS está centralizado?

"¿Se está consolidando el tráfico de Internet? Es decir, ¿está moviéndose hacia una fracción más grande del tráfico que involucra a solo un pequeño conjunto de grandes proveedores de contenido, redes sociales y plataformas de distribución de contenido? Parecería que sí, aunque sería recomendable contar con una mayor investigación sobre este asunto".

> -- Junta de Arquitectura de Internet sobre la Consolidación, en marzo de 2018

Pide y recibirás... O, como dicen los académicos: pide investigaciones, y al cabo de dos años, puede que tengas la suerte de recibir pruebas iniciales que potencialmente respondan a tu pregunta.

En 2018, cuando el despliegue de protocolos cifrados suscitó preocupaciones sobre la consolidación de consultas DNS en manos de unas pocas importantes empresas privadas, no había muchas pruebas que demostraran cuán concentrado ya estaba el mercado. Durante los últimos dos años, ha habido mucha más evidencia que respalda esta hipótesis. En la reunión del Grupo de Investigación de Mediciones y Análisis para los Protocolos (MAPRG) durante la IETF109, Sebastián Castro presentó un documento titulado *Clouding up the Internet: how centralized is DNS traffic becoming?*, que fue publicado en los procedimientos de la Conferencia de Medición de Internet de ACM en 2020.

El enfoque de los autores se basa en analizar el tráfico DNS que viaja desde los resolutores hacia tres servidores autoritativos: uno en los Países Bajos (.nl), otro en Nueva Zelanda (.nz) y el último en B-ROOT (múltiples dominios de nivel superior). El conjunto de datos final analiza las consultas de una única semana en tres años diferentes, que resulta con información sobre 55.000 millones de consultas DNS. Luego, se identifica el tráfico proveniente de las cinco grandes empresas (Google, Amazon, Microsoft, Facebook y Cloudflare) involucradas en la provisión de servicios de alojamiento.

En comparación con .nz y B-ROOT, el servidor autoritativo .nl experimentó la mayor concentración de tráfico recibido: más de un tercio del tráfico provenía solamente de estas cinco empresas, con Google a la delantera. La gran porción de tráfico de Google se puede explicar, en parte, por el hecho de que solo Google y Cloudflare de estas cinco empresas operan con resolutores DNS públicos. Los autores también identificaron que las consultas de resolutores DNS públicos eran mayoría en el conjunto de datos.

Al mismo tiempo, puede que estos datos por sí solos no sean suficientes para capturar la concentración dentro del mercado DNS. Por ejemplo, no responden la pregunta de si existe una cantidad comparable de proveedores de servicios de Internet (ISP) que sean responsables directos o indirectos de niveles similares de tráfico hacia servidores autoritativos. Sin embargo, dado que estas cinco

empresas están involucradas en la provisión de alojamiento de otros servicios, los resultados de este documento muestran niveles preocupantes de consolidación en la economía de Internet en general.

Cabe también recordar que el enfoque de los autores se basa en la medición de tráfico desde resolutor hacia servidor autoritativo; es decir, este análisis no es representativo de cuán consolidado está el mercado del lado del usuario. Teniendo en cuenta que los resolutores de Google o Cloudflare cachean las respuestas (y se las brindan a usuarios sin contactar a los resolutores autoritativos en cada instancia individual), el tráfico DNS del usuario al resolutor puede ser incluso más concentrado que lo que indican los hallazgos del documento.

Ese caso coincidiría con los resultados del documento de Roxana Radu y Michael Hausding, titulado *Consolidation in the DNS resolver market – how much, how fast, how dangerous?*, publicado en la edición de febrero de la revista Journal of Cyber Policy. A partir del análisis de 100.000 mediciones de la base de datos del Observatorio Abierto de Interferencia de la Red (OONI), los autores concluyeron que "existe una alta concentración de poder en manos de Google y Cloudflare, que controlan la mitad de la totalidad del mercado".

Además de que estas son malas noticias para quienes buscan más competencia en sus mercados digitales, las consecuencias respecto de la seguridad y la privacidad en la consolidación del mercado DNS también son significativas. Los grandes proveedores de DNS pueden ser excepcionales puntos de falla, como lo probó el ataque de denegación de servicio a Dyn en 2016, que resultó en la indisponibilidad de varios servicios importantes en Europa y América del Norte. A la naturaleza sensible de las consultas DNS también la pueden explotar las empresas para su ventaja comercial, ya sea mediante la venta de conjuntos de datos o para ayudar a sus servicios de publicidad microfocalizada.

Es probable que el despliegue de protocolos de DNS cifrado, como DNS sobre TLS (DoT) y DNS sobre HTTPS (DoH), atrinchere esta tendencia, considerando que Cloudflare y Google son actores influyentes en la imposición de dichos protocolos a los usuarios finales. Si bien los reguladores alrededor del mundo están poniéndose rápidamente al día con las preocupaciones sobre la competencia en la economía de Internet, esta evidencia reciente es un aviso claro para que los formuladores de políticas presten más atención a la consolidación del mercado en las partes "invisibles" de nuestras redes. De todos modos, siempre tienen la opción de solicitar que se hagan más investigaciones.

VI. Censores transparentes y otras extensiones de códigos de error extendidos

El WG del DNS en el IETF continúa expandiendo su base de códigos DNS con las nuevas funciones y mejoras a las funciones previas. En la sesión más reciente, una propuesta sobre espacio privado en el DNS con códigos de dos letras recibió opiniones mixtas, mientras que el trabajo en políticas sobre las consecuencias operativas del DoH aún no es bienvenido.

Todas esas consultas DNS fallidas

Con las especificaciones técnicas actuales para el DNS, recibir un mensaje de error en respuesta a una consulta DNS puede significar varias cosas. La nueva RFC 8914 sobre Códigos de Error Extendidos propone cambiar esto para que los administradores puedan ser capaces, al menos, de conocer los detalles específicos de un error.

Entre los diferentes problemas con los que se puede topar una consulta, y sobre los que un administrador debe tener conocimientos para poder tomar las contramedidas necesarias, se encuentran los problemas con los certificados de DNSSEC (por ejemplo, certificados vencidos, firmas que aún no son válidas o incluso algoritmos de cifrado no compatibles), problemas de red o problemas de *upstream* con los servidores autoritativos del dominio. Las consultas también pueden fallar debido a razones de políticas; por ejemplo, si un resolutor o un servidor autoritativo se encuentra en una jurisdicción que establece requisitos de bloqueo, filtrado o prohibición para la resolución de consultas. La lista con 26 códigos de error en la RFC 8914 diferencia meticulosamente estos casos.

Sin embargo, no bien terminó de publicarse la RFC 8914, un grupo de editores de McAfee, Open-Xchange, Citrix y Orange solicitaron mayor transparencia con respecto a la "categoría de filtrado y bloqueo".

En base a la actual lista de códigos de error, los usuarios no saben por qué un dominio fue filtrado o bloqueado, según explicó Tirumaleswar Reddy durante la sesión de DNSOP en la reunión IETF109. Reddy y sus coautores proponen una opción de DNS extendido (EDNS(0)) que devolvería un identificador de recursos uniforme (URI) que explique la razón por la cual la consulta DNS se filtró. Algunos beneficios predecibles incluyen la capacidad de que los usuarios finales envíen objeciones oportunas a las partes responsables cuando un contenido que debería estar disponible no lo está.

Sin embargo, la solución propuesta acarrea problemas de seguridad considerables, en particular la inyección maligna de una página de error por parte de un atacante. Reddy, cuyo *draft* ya identifica este problema, prometió que el *draft* intentaría solucionar esto haciendo obligatorio el cifrado del DNS y forzando

el rechazo de cualquier opción URI EDNS(0) provista por orígenes no autenticados.

Con tales limitaciones, la implementación de mensajes de filtrado transparentes puede volverse bastante restringida, según indicó el académico estadounidense Wes Hardaker, y recomendó esperar para ver si los Códigos de Error Extendidos de la RFC 8914 tendrían una mayor adopción antes de dar los siguientes pasos. También propuso que se podría usar, entretanto, un campo de texto libre, que esté limitado en longitud, para señalizar el URI de una página de error explicativa.

Señalizar errores en la otra dirección

Dos empleados de ICANN, Roy Arends y Matt Larson, también quisieron señalizar los errores hacia los servidores de nombre autoritativos que estén atravesando el problema.

Un agente informador para el dominio autoritativo, especificado en la opción EDNS(0) recibida del servidor autoritativo, podría obtener indicaciones de las consultas relacionadas con el error a través de resolutores recursivos, según propuso Arends.

Tal propuesta suscita preocupaciones de seguridad similares a las de Reddy y sus coautores, pero Arends parece decidido a seguir adelante. Tras los debates en el WG de DNSOP, observó que el documento del IETF está actualmente clasificado como un documento de presentación independiente, por lo que no sería necesario que el WG lo adopte.

Zonas privadas por nombre y no solo por número

Como se informó previamente en el documento *CENTR Tech Trends Watch Q2/2020*, Arends también propuso, junto con Joe Abley, la creación de una lista administrada por el IETF de espacios de nombres privados de dos letras siguiendo los códigos de dos letras en las normas ISO 3166-1. Esta propuesta generó gran tráfico en la lista de correo electrónico desde el primer trimestre, y ahora llegó a la reunión de DNSOP. Algunos miembros del WG como Ted Hardie, expresidente de la IAB, advirtieron que este problema debía ser debatido entre ICANN e ISO.

Se terminó la discusión: ¿una nueva edición en DNSOP?

Con el WG del DoH cerrado, los autores de un *draft* sobre pautas para los operadores están buscando con desesperación un nuevo espacio al cual dirigir su trabajo. Sin embargo, los presidentes de DNSOP ciertamente desean mantener los cargados debates políticos fuera del WG tanto como puedan. Para saber más sobre la disputa continua sobre el DoH, el descubrimiento y los problemas de privacidad relacionados, esté atento al próximo posteo de blog de CENTR.

VII. ¿La diversidad a toda costa? El IETF busca un nuevo presidente

La búsqueda actual de un nuevo presidente del IETF ofrece a la comunidad la oportunidad de revisar los problemas de diversidad y elegir un candidato que cuente con el auspicio de uno de los participantes más nuevos en el proceso de estandarización. Lamentablemente, el candidato más plausible desde el punto de vista de la diversidad está auspiciado por el proveedor chino Huawei, que está actualmente en guerra comercial con EE. UU.

Huawei ya envía más desarrolladores al IETF que la mayoría de los participantes de larga data en la estandarización de Internet. Para la reunión IETF109, Huawei y su subsidiaria Futurewei inscribieron a 92 asistentes, mientras que Cisco, uno de los auspiciantes más antiguos del IETF y empleador de la actual presidenta, Alissa Cooper, inscribió apenas a 66 personas. Según las estadísticas de Cooper para la reunión IETF109, las empresas y universidades chinas se hicieron presentes para convertirse en el segundo grupo de participantes más numeroso tras la cohorte de participantes estadounidenses.

Dos candidatos para el puesto de presidente, Barry Leiba y Alvaro Retana, son empleados de Futurewei, la subsidiaria de Huawei centrada en la investigación, y un tercer candidato, Adrian Farrel, ubicado en el Reino Unido, es conocido también por haber cooperado con Huawei en numerosos proyectos. En el período previo a la elección, queda claro que Huawei busca auspiciar su primer presidente del IETF.

Puestos de tiempo completo

El puesto de presidente del IETF es casi un trabajo de tiempo completo. Las tareas incluyen supervisar el trabajo del IETF en general y el del IESG, el organismo par del IETF, en particular. El presidente del IETF es director del flujo de trabajo del Área General, que tiene tareas similares a la reciente separación de la Internet Society. Además, el presidente del IETF debe representar al IETF en el mundo exterior, así como también en varios organismos relacionados con la gobernanza de Internet.

IETF LLC, la organización formalmente encargada de llevar a cabo las reuniones del IETF y la infraestructura intersesional, no remunera este puesto, por lo que quienes tomen el rol deben obtener sustento financiero por parte de sus empleadores o socios de la industria. Históricamente, uno de los auspicios más curiosos fue el de la Agencia Nacional de Seguridad de los Estados Unidos para el presidente Russ Housley entre 2007 y 2013.

Clima anti-Huawei

Si autoridades públicas de EE. UU. han auspiciado previamente a presidentes de manera directa y el IETF tiene la intención de mejorar la diversidad en su representación, ¿por qué no habría de haber un jefe del IETF auspiciado por Huawei?

Para el Comité de Nominaciones del IETF, formalmente responsable de seleccionar candidatos calificados para puestos importantes, es verdaderamente una complicación el fuerte prejuicio político contra Huawei y otros proveedores chinos por parte de EE. UU. y algunos de sus aliados. Este prejuicio se evidencia claramente tanto en las sanciones comerciales como en las listas de entidades de EE. UU., así como también en algunos países de la Unión Europea. Otra instancia de este prejuicio es la Iniciativa Red Limpia del Departamento de Estado de EE. UU.

Un participante estadounidense observó que el IETF no se rige por la regulación de EE. UU., por lo que no emergerían problemas jurídicos. Sin embargo, según este experto del IETF de larga data, podría ser un problema desde la perspectiva política si algún militante del congreso quisiera armar un escándalo. Y, a pesar de que pronto habrá un cambio en el mandato del Departamento de Estado, la histeria anti-China podría permanecer debido a que el presidente entrante podría actuar con cautela, aunque solo sea para rechazar los gritos de “marioneta de China”.

Los siguientes se encuentran en la lista de candidatos:

- Adrian Farrel, Old Dog Consulting
- Alvaro Retana, Futurewei
- Barry Leiba, Futurewei
- Deborah Brungard, AT&T
- Fred Baker, consultor, miembro del directorio de ISC, y expresidente del IETF
- Lars Eggert, NetApp
- Rich Salz, Akamai

VIII. Transporte del DNS: ¡empezó la carrera!

No uno, ni dos, sino tres protocolos nuevos ofrecen opciones de capa de transporte de Internet para el Sistema de Nombres de Dominio (DNS). De todas maneras, no debemos perder de vista a la última generación. A continuación, presentamos un rápido vistazo al catálogo de opciones de DNS sobre TLS (DoT), DNS sobre HTTPS (DoH) y DNS sobre Quic (DoQ).

Mejor seguridad en el destino final

La seguridad del transporte del DNS se está volviendo muy popular. Mozilla apretó el paso cuando anunció en 2019 la implementación de DNS sobre HTTPs (DoH) basado en el navegador en EE. UU. Microsoft, Google y Apple siguieron el ejemplo de anunciar implementaciones, al igual que operadores de red como ComCast, que se asoció a Mozilla el verano pasado.

Tampoco escasean quienes implementan DoH en el lado del operador de red en Europa. Tanto Deutsche Telekom como British Telecom están implementando esa opción. Según Nicolas Leymann, el operador de red alemán ofrecerá DoH experimental para sus clientes durante el primer trimestre de 2021.

En un principio, el candidato favorito para una solución amigable con la privacidad era DNS sobre TLS (DoT). Aún se considera como la evolución natural para incorporar seguridad a la infraestructura del DNS y deja los parámetros de configuración de servicio en manos de los usuarios y los proveedores de red. Comparado con el DoH, el DoT padece el hecho de que el tráfico DoT es fácilmente discernible, debido a que se ejecuta bajo un número de puerto especial.

En una columna reciente sobre las tendencias del DNS, el director científico de APNIC, Geoff Huston, también señala otro problema: el DoT no elimina el potencial de manipulación de las respuestas DNS, sino que confía en el proveedor DNS de preferencia. En palabras de Huston: “Lo único que sabemos es quién nos miente”.

Los candidatos

Usando el transporte web HTTPs como base, las consultas DNS se benefician del cifrado TLS. También se vuelven parte del inmenso flujo de tráfico HTTPs y no es fácilmente identificable por parte de las redes. Los ingenieros de Mozilla jamás se cansan de incluir estos beneficios de privacidad para los usuarios. Usar DNS DoH se vuelve parte de la aplicación y permite que las aplicaciones esquiven redes remotas y locales, así como también plataformas.

La creación más reciente es Oblivious DoH (ODoH), promocionado por Cloudflare como la respuesta definitiva a las preocupaciones sobre la concentración de la información del usuario. ODoH añade un *proxy* entre el resolutor público y el usuario final, separando la información del DNS del IP del usuario.

Durante la reunión IETF109, Christian Huitema, experto en privacidad por diseño, preguntó al WG de DNS Privacy (DPRIVE) si podría continuar con el protocolo número tres de seguridad del DNS, DNS sobre Quic (DoQ).

Con Quic, el nuevo protocolo de transporte del IETF, en la línea de llegada, el DoQ se podría adoptar ahora seriamente. Quic se basa en UDP e integra la pila de TLS

para convertirse en el primer protocolo de transporte que preserva la privacidad de forma nativa. Muchos creen que será un gran competidor de TCP. Lo que podría hacer atractivo al DoQ para los proveedores de DNS es que el cifrado se aborda a nivel del transporte. Además, el DNS podría beneficiarse de funciones adicionales de Quic, como la multiplexación.

¿Uno para gobernarlos a todos?

Si bien Huston no prevé un gran futuro para DoT y también considera que el casi olvidado Datagram TLS (DTLS) basado en UDP (el cuarto protocolo de transporte de DNS seguro) es demasiado frágil, otros expertos piensan que existe una posible división del trabajo entre los candidatos.

Sara Dickinson, experta en privacidad del DNS de la empresa consultora británica Sinodun, afirma que "tendremos múltiples protocolos con áreas especializadas".

Considera que el DoH es el preferido de las aplicaciones, mientras que el DoT tiene más sentido para los resolutores *stub* básicos. Piensa, además, que para el DoQ, que llegó tarde al juego, no hay demasiado apetito, al menos para la ruta entre el resolutor *stub* del usuario y los resolutores recursivos del proveedor. Por otro lado, Dickinson espera que la ruta entre los resolutores recursivos y autoritativos esté cifrada, ejecutando DoT o DoQ. El WG de DPRIVE acaba de empezar a trabajar en la seguridad de la parte más alta de la ruta de resolución del DNS. No tienen en cuenta al DoH para esta tarea.

A la larga, puede que la velocidad sea el factor decisivo. "Pienso que el DoQ deberá probar que es más eficiente para que sea elegido antes que el DoT para desempeñar ese rol, ya que la comunidad del DNS está bastante cómoda con el DoT por ahora". Sin embargo, otras voces señalan que el DoQ aún tiene posibilidades de vencer al DoT, incluso para la ruta de resolutores *stub* a recursivos, ya que puede que sea más fácil de usar.

La sobrecarga de los despliegues paralelos

Para quienes llevan a cabo las implementaciones, es difícil decidir en quién invertir el dinero. Existía cierto riesgo de que uno de los candidatos se volviera dominante y que los esfuerzos por desplegar los demás protocolos fueran inútiles, según lo advirtió durante la reunión IETF109 Wes Hardaker, del Instituto de Ciencias de la Información de la Universidad de California del Sur (USC/ISI). Aun así, elegir un ganador por anticipado no ha sido el método preferido en el IETF últimamente.

Además, los ejecutores en Deutsche Telekom están felices de desplegar al menos DoH y DoT en paralelo por el momento, mientras esperan la llegada de DoQ. La carrera ya empezó...

IX. Elegir los resolutores correctos para el DNS cifrado: ¿quién descubre las opciones?

El WG de ADD del IETF ha estado intentando ponerse al día con el despliegue del DNS cifrado y se reunió en seis ocasiones el año pasado. Su objetivo es brindar medios estandarizados para descubrir qué opciones cifradas están disponibles para diferentes usuarios de red y un medio para que dichos usuarios seleccionen la opción más adecuada para el uso deseado. Este trabajo implica maniobrar entre tareas técnicas y decisiones de políticas que otros WG, como el de DNSOP, se muestran reacios a asumir.

Las consultas DNS son invisibles para la mayoría de los usuarios de Internet. Normalmente, la consulta para mapear un nombre de dominio a un servidor se envía a través de un navegador web a un resolutor cuando un usuario intenta visitar una dirección web. En muchos lugares, los servicios de resolutor esenciales han sido operados por los proveedores de red, a menos que el usuario haya indicado específicamente que quiere un servicio de resolutor diferente. Ni los proveedores de red ni los del DNS han hecho grandes intentos por educar a los usuarios en temas de privacidad en este arreglo, así como tampoco tuvieron prioridad en la agenda las fallas de privacidad en los protocolos subyacentes hasta después de 2013.

No obstante, con una creciente ola de prioridades de privacidad y seguridad para las infraestructuras más fundamentales de Internet, los proveedores de servicios lanzaron varias iniciativas de DNS cifrado. Parece ser que el mensaje es que la elección de una solución de DNS seguro y privado debería ser tan fácil como la decisión de permitir o prohibir que un navegador acceda al micrófono o la cámara.

El descubrimiento de resolutores cifrados equivalentes

Un *draft* propuesto por ingenieros de Apple, Cloudflare y Microsoft está dando sus primeros pasos con el "Descubrimiento de resolutores cifrados equivalentes" (DEER). Su objetivo es brindar dos mecanismos para subir de nivel a clientes hacia resolutores DNS cifrados.

El primer mecanismo se basa en consultar un dominio especial en el TLD .arpa para buscar resolutores DNS cifrados. El segundo toma lugar cuando la aplicación del usuario ya conoce el nombre del *host* de un servidor DNS cifrado. Para el segundo caso, un nuevo tipo de registro de recurso (SVCB) transmitirá información en el protocolo de cifrado y los puertos bloqueados.

El WG de ADD aún no adoptó la propuesta; nada es fácil cuando se trata del DNS cifrado. En un debate que duró dos horas, el WG intentó definir si el concepto de

“equivalencia” en “resolutores cifrados equivalentes” se limita a las consultas, las respuestas, los conjuntos de nombres, los requisitos de rendimiento o las leyes.

Harald Alvestrand, expresidente del IETF e ingeniero en Google, recomendó no hacer ninguna afirmación sobre dicho concepto en el DEER. En su opinión, a la larga, el DEER contiene mecanismos para brindar recomendaciones a los usuarios finales sobre los servicios de DNS cifrado y los usuarios finales son capaces de decidir por sí mismos cuán similares o diferentes quieren que sean sus servicios DNS.

Privacidad, legislación y expectativas del usuario

Muchos expertos señalaron que el uso generalizado del DNS no cifrado en las redes domésticas de los usuarios implica una carencia de expectativas de privacidad *a priori*. Encender el cifrado del DNS representaría un beneficio neto para ese gran grupo de usuarios, que usualmente no tiene conocimiento alguno sobre el DNS.

Una mirada opuesta es que los usuarios han decidido confiar en sus proveedores de red, incluso mediante debates sociales de larga data sobre el control del contenido y la responsabilidad legal. Enviar sus consultas a un proveedor tercero cambiaría la ecuación.

Equilibrar los intereses comerciales y sociales vinculados con el manejo de la información sigue siendo un problema para la comunidad de estandarización de Internet. Si bien nuestras infraestructuras de red en común se están haciendo cada vez más robustas contra las amenazas a la privacidad y la seguridad, la dinámica de poderes que ha reinado desde los comienzos de la década de 1990 se está poniendo a prueba con el despliegue de nuevas soluciones técnicas por parte de nuevos actores comerciales. Incluso cuando la salvaje web atrae nuevamente críticas del comisionado Thierry Breton, entre otros, también es cierto que siempre que dejemos que rija la tradición, todos sabremos con qué estaremos lidiando.

Sobre los autores:

Gurshabad Grover es tecnólogo e investigador jurídico ubicado en Bangalore, India, donde se desempeña como investigador sénior para el Centre for Internet and Society. Gurshabad escribe principalmente sobre temas de seguridad en la red, privacidad y censura.

Monika Ermert se ha desempeñado como periodista de tecnología de la información durante más de 20 años. Cubrió el cambiante panorama de la gobernanza de Internet, los intentos de regulación de la UE y el resto del mundo, y los riesgos y las ventajas de la tecnología. Tiene una maestría en estudios de medios/chino de la Universidad de Tubinga y reside y trabaja en Múnich, Alemania.