Informe de CENTR

IETF 102

Montreal, 14 - 20 de julio de 2018

Traducción - LACTLD

LACTLD agradece 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
Latin American and Caribbean ccTLDs Organization

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

Aspectos destacados

Del DNS al DNS sobre TLS y DNS sobre HTTPS: ¿hacia el DNS sin resolutor?

El *draft* para el DNS sobre HTTPS (DoH, por sus siglas en inglés) está a punto de llegar al IESG (actualmente *draft* AD) para su revisión final y la última llamada del IETF. Ahora emergen algunas preguntas interesantes ante las comunidades del DNS y HTTP: ¿convivirán el DNS, el DNS sobre TLS y el DoH? Más específicamente, ¿el DNS se convertirá, en gran medida, en una aplicación web? O, como preguntan algunos pesimistas: ¿los buscadores y las redes de distribución de contenidos (CDN, por sus siglas en inglés) podrán opinar sobre qué TLD debería ser resuelto? Al final, ¿la web conquistará la Internet?

El IETF en Montreal no mantuvo otra sesión de WG sobre DoH, pero sí tuvo lugar una reunión BoF fuera de los WG sobre «Identificación y uso de resolutores DNS» (DRIU, por sus siglas en inglés), junto con dos reuniones paralelas no registradas (BoF de bar) sobre SRV y HTTP, y DNS sin resolutor, en la que se debatieron cuestiones relacionadas.

El debate más controvertido se desarrolló en torno al *draft* «DoH Digest» de Mark Nottingham, el cual fue presentado en la BoF sobre DRIU. Básicamente, la idea de Nottingham apunta a cambiar el modelo DoH actual con respecto a los servidores DoH preconfigurados. En lugar de tener solamente un servidor DoH configurado —este es el modelo actualmente implementado por Mozilla/Cloudflare—, los clientes tendrían la posibilidad de elegir entre varios servidores.

Mozilla describe el contrato Mozilla-Cloudflare como una combinación de resolutores de confianza más el DoH. Las consultas cifradas incorporadas en HTTPS llegan desde los usuarios de Firefox a Cloudflare, que aprovecha su gran infraestructura de DNS para devolverles las respuestas DoH a los usuarios. Algunos habían anticipado esta tercerización de la provisión del DoH.

DoH Digest

Nottingham reiteró las ventajas del DoH desde el punto de vista de la comunidad web: la privacidad y la fiabilidad gracias al cifrado y a que actúa con una sola de las partes (no recurre a terceros operadores del DNS). También se podría mejorar el desempeño mediante la combinación del HTTP Client y el DNS Client, y el uso de la información en el flujo de solicitudes DNS para acumular todo su tráfico en una menor cantidad de conexiones (posiblemente solamente una), permitiendo así una mejora en la coordinación del control de la congestión y evitando los costos de configuración de conexión. Nottingham también prevé el uso potencial de los certificados secundarios (de httpsBis).

La idea de Digest, según Nottingham, se basa en que «*cada servidor DoH que el cliente configure enviaría un digest al navegador (a través de medios a debatir), y ese digest sería usado como una pista para la solicitud que ese servidor DoH querría ver. [...] Si (un navegador) Mozilla habilitara esto, su navegador sería configurado con una cierta cantidad de servidores DoH; cuando se conecte con cada uno, recibiría un* digest*, y usaría eso como contribución para tomar la decisión sobre qué servidor DoH usar para una solicitud dada*».

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

Nottingham se refirió a la propuesta como una primera lluvia de ideas. También reconoció el riesgo de concentración, que fue destacado durante la BoF por el expresidente del IETF, Jari Arkko. Nottingham escribió, en un email, a quien escribe: «*Aquí hay una negociación. El DoH funciona mejor para evitar la censura cuando está coubicado con un servidor Web popular; por ejemplo, un gran sitio Web o una CDN. Sin embargo, no queremos darles a los grandes sitios Web o a las CDN más ventajas sobre los sitios pequeños, entonces podríamos intentar idear algún otro mecanismo que no exija un acuerdo previo con el navegador. Eso todavía no se ha debatido*».

Como reacción tras la BoF, el presidente de la IAB, Ted Hardie, dijo que el incentivo de seleccionar a partir de una variedad de servidores DoH era «mediocre» con el dispositivo local que ya tiene un buen upstream con una sesión TCP/TLS/HTTP establecida «y querrá evitar la latencia del establecimiento de sesión del balanceo de carga en muchos casos». Hardie, a diferencia de otros colegas de Google, dijo que, para atraer tráfico de solicitudes destinadas a su red, un servidor DoH necesita «un gran caché, buenas conexiones a otros servicios DNS, todo el paquete».

«*Creo que, en definitiva, este es un modelo en el que el usuario no tiene control sobre dónde van las solicitudes y el sistema heurístico que subyace acaba enviándolas a un sitio dispuesto a ofrecer el mayor número de nombres (rutas más específicas) y la infraestructura de consultas DNS más grande. Eso terminará detrás de unas pocas CDN, a menos que esté equivocado*», dijo Hardie.

El DNS sobre HTTPS sobrepasa al DNS sobre TLS

A pesar de las preocupaciones sobre el DoH y la idea “Digest”, el DoH parece ser, actualmente, la tecnología que funciona de manera más rápida que DNS sobre TLS (DoT). Este último, ya estandarizado, habría sido una alternativa más de conformidad con el sistema DNS tradicional y vendría con al menos la opción para operaciones DNS descentralizadas (aunque la concentración en 8.8.8.8, 1.1.1.1, y 9.9.9.9 está en progreso).

Patrick Mc. Manus, de Google, explicó el razonamiento detrás de la preferencia del DoH desde la perspectiva del desarrollador Web en una publicación en mayo:

«*Las implementaciones del DoH, en virtud de también ser aplicaciones HTTP, tienen fácil acceso a una cantidad enorme de infraestructura común con la cual impulsar despliegues. Algunos ejemplos son las CDN, cientos de bibliotecas de programación, bibliotecas de autorización, proxies, balanceadores de carga sofisticados, servidores de alto volumen, y más de mil millones de motores Javascript desplegados que ya tienen interfaces HTTP (también vienen con un modelo de seguridad razonable [CORS] para el acceso a fuentes detrás de cortafuegos). El DoH incluye también inherentemente la negociación de contenido HTTP —permitiendo que expresiones nuevas de datos DNS (json, xml, etc.) se desarrollen en entornos de programación no tradicionales*».

Sara Dickinson, de Sinodun, compartió algunas percepciones sobre la carrera entre la comunidad web y la comunidad DNS en una entrevista publicada en el blog de CENTR. Durante el IETF, Dickinson brindó una versión breve de la charla que dio en la Cumbre de la División Global de Dominios de ICANN en la que presentó el panorama de la carrera DoH/DoT.

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

Dickinson también fue autora de un nuevo documento que solicita un perfil especial para el uso del DoH con el objetivo de mitigar los riesgos de privacidad relacionados con el DoH. Escribió que las nuevas preocupaciones sobre la privacidad resultan del mero hecho de que el nuevo transporte (comparado con el DNS sobre UDP, TCP o TLS [RFC7858]) incluye identificadores de clientes (por ejemplo, user-agent, accept-language) que no están presentes en ningún transporte DNS existente. Todavía se debate cómo mitigar esto de la mejor manera. Aunque Dickinson recomienda, por ejemplo, que «los clientes de DoHPE *deberían* enviar consultas sobre conexiones usadas solamente por DoHPE ("conexiones dedicadas al DoHPE") para evitar mezclarlas con tráfico HTTPS que puede contener mensajes HTTPS con identificadores de clientes», otros ingenieros señalan que usar conexiones dedicadas puede ayudar, en cambio, al análisis del tráfico.

Comunidades DNS y Web: ¿cooperar o competir?

Se solicitó cooperación adicional entre las comunidades Web y DNS en el WG de DNS (ver más abajo) y en las dos BoF de bar. Una fue el debate sobre SRV y HTTP sobre la ubicación de servicio. El CNAME utilizado para usar bigbank.example en lugar de www.bigbank.example fue una exageración, según los expertos, porque el CNAME cambia la dirección de las búsquedas DNS y, con frecuencia, deja la zona. Se decidió que la idea de usar registros SRV en cambio para expresar qué servidores brindarán un sitio no era óptima debido a problemas con los *wildcards*. Ahora, la gente de la Web y el DNS busca otros candidatos potenciales para resolver el problema de something@apex. Los presidentes del WG de DNSOP armarán una lista de correos específica. Según Olafur Gudmundson, uno de los candidatos puede ser un «HTTPS RRtype que tenga los servidores y la información de SNI+KEY en el registro ya que a ese registro se le puede añadir información».

La segunda reunión BoF donde se juntaron los expertos web y DNS versó sobre el «DNS sin resolutor». Según algunos espectadores, se basó en «el uso de un resolutor fuera de red sobre un protocolo al azar en lugar de un resolutor DNS provisto por la red».

Según Dickinson, la gente del DNS, de alguna manera, tuvo la culpa del desarrollo del DoH (vea la entrevista) al no abordar algunos de los problemas a los que la comunidad web quería poner fin. Para el DNS, el gran traslado al Puerto 443 podría resultar en un cambio considerable en su entorno.

IASA 2.0 y la búsqueda espiritual del IETF

El IETF está avanzando en su nueva estructura administrativa y se está volviendo un poco más independiente. Sin embargo, se mantienen las preocupaciones sobre cómo continuar atrayendo suficientes ingenieros para que participen —y, por lo tanto, también sobre cómo recaudar los fondos necesarios para financiar las actividades del IETF, la secretaría, los costos de las reuniones, y la serie de RFC. Un debate iniciado por la IAB sobre el futuro de la serie de RFC bajo el título RFCPlus arrojó algo de luz sobre la búsqueda espiritual.

IETF LLC

Durante la sesión plenaria en Montreal, la presidente del IETF, Alissa Cooper, anunció que, para finales de agosto, el IETF espera haber establecido formalmente una nueva Limited Liability Company (Sociedad de Responsabilidad Limitada). La Administración de la LLC del IETF se

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

convertirá en la «sede empresarial del IETF, la IAB y el IRTF», dijo Cooper. Permitirá que el IETF celebre contratos con los operadores de la secretaría de manera independiente, se reúna con los hoteles y contrate al personal.

Con la reforma conocida como IASA 2.0, el IETF pasará a ser una «entidad separada» de la ISOC, compartiendo el estatus de exención de impuestos de ISOC (como una organización sin fines de lucro 503c según las leyes de EE. UU.), basada en Delaware, EE. UU. Para aquellos que estén interesados en más detalles, se abrirá un periodo de comentarios sobre los documentos jurídicos por un tiempo corto en agosto, según la presidente del IETF.

Se afirmó que se mantiene estrecha la relación entre el IETF y la ISOC. Esta última se reserva algunos derechos, especialmente para aprobar:

- Enmiendas al Acuerdo LLC.
- Cambios fundamentales y significativos en la naturaleza de las actividades de la LLC.
- Cambios significativos en las políticas de contabilidad y tributarias acordadas previamente.
- La admisión de nuevos miembros, fusiones, la venta de todos los activos de la LLC, etc.
- La conversión de la LLC a otra forma de entidad jurídica.

En un intento por realizar una transición inmediata hacia la nueva configuración estructural, la ISOC contribuirá con fondos extra de 5 millones de dólares anuales durante los próximos tres años, además de su contribución anual habitual de 2 millones de dólares. Adicionalmente, el dinero que proviene de las Donaciones IETF (IETF Endowment) será transferido (2.6 millones de dólares en 2018).

	2018	2019	2020
Revenue			
ISOC annual contribution	$2,692	$5,000	$5,000
ISOC in-kind	315	0	0
Meeting revenue	3,909	4,154	4,219
In-kind revenue	113	35	35
Total	**$7,029**	**$9,189**	**$9,254**
Expenses			
Meeting expenses	$3,089	$3,172	$3,215
RFC services	1,238	1,262	1,198
IETF secretariat	1,375	1,404	1,436
Operating costs	670	1,564	1,795
ISOC support	315	0	0
Transition costs	75	0	0
Special projects	50	50	50
Tools	217	221	226
Total	**$7,029**	**$7,674**	**$7,920**
Net surplus		**$1,516**	**$1,334**

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

De la IASA 1.0 a la IASA 2.0: La nueva estructura administrativa

La reunión en Montreal fue sede de la última reunión del Comité de Supervisión Administrativa del IETF (IAOC), el organismo establecido durante la primera reforma del IETF. Iniciada por el entonces presidente del IETF, Harald Alvestrand (en ese momento en Cisco, ahora en Google), la IASA 1.0 (establecida en 2005) resultó en la primera formalización del trabajo administrativo, la introducción del puesto del Director Administrativo del IETF (IAD) y, algún tiempo después, la Fundación IETF.

Con la IASA 2.0, solo permanecerá la Fundación IETF (con algunas adaptaciones menores). Generalmente, la LLC debe encargarse de apoyar las operaciones en marcha del IETF (actividades vinculadas a las reuniones y otras no vinculadas a ellas), administrar las finanzas y presupuestos del IETF, la recaudación de fondos y la observancia («establecer y hacer cumplir las políticas para asegurar la observancia de leyes aplicables, regulaciones y normas»).

El Consejo LLC desempeñará el rol de supervisión y contratará al director ejecutivo de la LLC, quien, a cambio, llevará a cabo las operaciones diarias (que incluyen la contratación de otros miembros del personal para el desempeño de actividades variadas, como la recaudación de fondos, la participación con la comunidad, y la comunicación).

Durante la sesión BoF de la IASA 2.0 en Montreal, tuvo lugar un debate extenso sobre el rol del Consejo LLC y sobre cuántos miembros debería tener ese nuevo órgano de supervisión. Algunos participantes advirtieron que un consejo muy numeroso podría causar un cambio gradual en los objetivos del organismo. Al final, el resultado fue un número fijo de cinco miembros, que incluye: el presidente del IETF, un miembro del Consejo de Administración de la ISOC, y tres miembros designados por el Comité de Nominaciones (NomCom) del IETF (la llamada comenzará el 16 de agosto). Además, el Consejo LLC mismo puede optar por elegir hasta dos miembros más para el Consejo, elegidos por este.

Nuevas tarifas para las reuniones

La reducción en el número de participantes continúa siendo una preocupación para el IETF. Con 1.020 asistentes, la reunión en Montreal estuvo menos concurrida que la de Praga, de hace un año. La presidente del IETF, Alissa Cooper, anunció un aumento en las tarifas, comenzando por aquellos que se inscriban de manera tardía:

Fee Type	Due Date	Deadline	Amount (USD)
Early Bird	17 Sept 2018	7 weeks prior	$700
Standard	22 Oct 2018	2 weeks prior	$875
Late & On-Site	9 Nov 2018	≤ 2 weeks	$1000

Otro experimento planeado para la reunión en Bangkok es la reducción de los días de reunión a cuatro (de lunes a jueves, o seis para aquellos que asisten a la popular Hackaton del fin de semana previo).

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

La evolución y búsqueda espiritual del IETF: El debate sobre las RFCPlus

Otra búsqueda espiritual tuvo lugar en una BoF iniciada por la IAB sobre los potenciales cambios en la serie de publicaciones de RFC. En un intento por evitar la confusión sobre la «marca» RFC, la IAB propuso el experimento de llamar a las RFC solamente «estándares IETF» en el futuro y buscar otra denominación para los documentos de la IAB, el IRTF y el *stream* de documentos independiente.

Con este cambio, los observadores externos y los usuarios de la serie de RFC evitarían mezclar los estándares IETF que pasaron por los procedimientos habituales de revisión de pares con aquellos documentos hechos por individuos. La propuesta fue rechazada categóricamente por una mayoría aplastante. Muchos de los participantes tildaron de injustificada a la BoF y de «bochornosa» a la falta de inclusión de la editora actual de las RFC, Heather Flanagan.

Hubo quienes argumentaron que la incapacidad de los usuarios externos de diferenciar entre una RFC y un estándar de Internet causa problemas. Por ejemplo, el RIPE NCC (Centro de Coordinación de Redes IP Europeas) mantuvo debates sobre los documentos borradores con respecto al esquema de numeración del IPv6, promovido por sus respectivos autores como RFC del IETF sin haber pasado por el proceso oficial de los estándares. Si bien no es urgente, es un problema, según Marco Hogewoning (de RIPE NCC). La tergiversación de documentos individuales o informativos puede acarrear problemas, por ejemplo, cuando aquellos fuera de los organismos o la industria piden su implementación.

Sin embargo, la mayoría advirtió en contra del cierre de otros *streams* y de delegar el control de las RFC al IESG exclusivamente. El problema de larga data de «no toda RFC es un estándar de Internet y no todo estándar de Internet es una RFC» podría abordarse como un problema educacional o quizás mediante un formateo innovador. Los cambios son complicados, según señalaron algunos, incluyendo con respecto a la divulgación, licenciamiento, y declaraciones de DPI.

Un problema más arraigado, según advirtieron varios participantes, es perder la calidad de los documentos. Algunas partes ejercerían presiones para hacer que una RFC entre a cualquiera de los *streams*, y luego aprovecharían la confusión pública en cuanto al estado de los documentos —estándar o solamente un documento informativo no revisado por los WG del IETF, según dijo la Directora de Área Mirja Kühlewind (ETH Zürich). Instó a que la comunidad del IETF pensara sobre este tipo de abusos del sistema e hiciera algo al respecto. Tras este debate altamente contencioso, la BoF cerró solamente con un solo próximo paso, que fue solicitar datos sobre el «problema de la confusión» a Flanagan.

REGEXT: ¿Búsqueda de RDAP para reemplazar al WHOIS suspendido?

El Grupo de Trabajo de las Extensiones de Protocolos de Registro bien puede ser uno de los grupos que podría ser cuestionado con respecto a sus procesos para elaborar documentos de estándares RFC en grandes cantidades sin mucha participación de la comunidad del IETF. Al estar básicamente dominado por un gran registro (VeriSign, con una pequeña cantidad de contribuciones por parte de tres o cuatro registros más), un solo registrador (GoDaddy) e ICANN, el WG siempre se encuentra carente de revisores en el flujo continuo de extensiones EPP especiales para la industria ICANN-Registro-Registrador. El conjunto de materiales publicados para los miembros del WG es enorme: contiene 346 páginas de documentos borrador (de los

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

cuales no todos son nuevos, sino que la mayoría todavía es una labor en curso). El mero volumen de propuestas a veces permite, al parecer, sacar adelante temas favorecidos por un grupo de expertos cerrado sin mucha participación de la comunidad más amplia del IETF.

Durante la segunda reunión, el presidente del WG, Jim Galvin, siendo el único presidente de hecho en las reuniones (con el copresidente Antoine Verschueren que usualmente participa de manera remota) reconoció que la comunidad de RegEXT es una comunidad muy pequeña y que hay una alta demanda de pastores (*sheperds*) de documentos (quienes no pueden ser los autores de estos). Al mismo tiempo, el WG está a punto de reformular su carta constitutiva, dándole al grupo un margen para involucrarse en temas de trabajo más amplios. Las preocupaciones sobre el potencialmente amplio alcance se tradujeron en la adición de media oración en la nueva carta constitutiva del WG para asegurar un freno al cambio gradual de objetivos: «El grupo de trabajo puede también, **previa consulta con su director de área a cargo**, ocuparse de trabajos relacionados con la operación de los registros de identificadores de Internet, más allá de los protocolos EPP y RDAP». Una buena cantidad de documentos de WG llegaron a la última llamada del IETF:

- Allocation Token Extension for the Extensible Provisioning Protocol (EPP),
- Registration Data Access Protocol (RDAP) Object Tagging,
- Extensible Provisioning Protocol (EPP) Organization Mapping,
- Organization Extension for the Extensible Provisioning Protocol (EPP)

Algunos pasaron la última llamada de WG y se acercan a la revisión del IESG:

- Extensible Provisioning Protocol (EPP) Domain Name Mapping Extension for Strict Bundling Registration
- Change Poll Extension for the Extensible Provisioning Protocol (EPP)
- Registry Fee Extension for the Extensible Provisioning Protocol (EPP)

Con estos documentos listos, y la reformulación de la carta constitutiva del WG que espera aceptación por parte del IESG, el WG podría estar buscando nuevos trabajos, según dijo Galvin. Muchos candidatos presentaron sus propuestas borrador en Montreal.

Galvin dijo que uno de los candidatos que podría avanzar de inmediato era la propuesta presentada por Roger Carney de GoDaddy que busca la automatización (tanta como sea posible) para los registradores en su intento por sumar nuevos registros. Carney señaló que le llevó a su empresa seis semanas procesar cuestionarios para los nuevos registros sobre su manejo de los aspectos compartidos del sistema de registros y las extensiones EPP. Con la propuesta Registry Mapping (mapeo de registro), se formalizará una reducción de verificaciones, disminuidas a dos páginas y permitirá lidiar con 80 por ciento de las preguntas en cinco minutos, antes de abordar el remanente 20 por ciento que no se automatiza fácilmente. Puede encontrar el borrador de la propuesta aquí. Scott Hollenbeck anunció que su empresa había presentado un reclamo de DPI sobre tecnología en el *draft*.

Aunque los asistentes retrocedieron frente a otra propuesta de Jim Gould de VeriSign sobre el problema de sincronización de los servidores y los clientes sobre un conjunto en común de características EPP compatibles, Gould anunció que volvería con una propuesta borrador para la consideración del WG.

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

¿La especificación temporaria de ICANN para el GDPR como base para hacer obligatoria la búsqueda de RDAP?

Para ICANN, Francisco Arias propuso varios temas de trabajo en los que el WG puede empezar a trabajar. Durante la sesión de trabajo más larga del lunes, Arias presentó la solicitud de ICANN sobre funciones de búsqueda de RDAP extendidas, en particular las siguientes opciones que actualmente no son soportadas por RDAP:

- Coincidencia parcial de *wildcard* en el comienzo.
- Compatibilidad para múltiples casos de *wildcard*.
- Compatibilidad para que los operadores lógicos «AND», «OR», «NOT» se unan a un conjunto de criterios de búsqueda a solicitud del cliente.
- Especificación explícita de los parámetros del patrón de búsqueda por ser utilizados en cada búsqueda de tipo de objeto.
- Mejoras en la internacionalización.

Es interesante que Arias apuntó a la especificación temporaria reciente para el GDPR como el documento que solicita que la búsqueda del RDAP sea ofrecida por los registros y también los registradores (además de webwhois). Scott Hollenbeck ofreció trabajos existentes sobre las expresiones habituales como el camino hacia rutinas de búsqueda más poderosas en el RDAP.

Un participante cuestionó el vínculo entre la especificación temporaria de ICANN y el cambio de Websearch a la búsqueda de RDAP, aunque Arias apuntó a un anexo en la especificación temporaria, la cual dijo que aplicará el cambio para las partes contratadas de ICANN. Andy Newton (ARIN) planteó las preocupaciones sobre el potencial abuso de las búsquedas («principalmente utilizadas en la minería de datos»).

Varios participantes también cuestionaron un segundo conjunto de propuestas de los expertos de ICANN, que cubrían el depósito de datos en un tercero (*data escrow*).

- Internet Domain Registry Data Escrow specification (draft-arias-registry-data-escrow).
- Registry Data Escrow Specification (draft-arias-noguchi-registry-data-escrow).
- Domain Name Registration Data (DNRD) Objects Mapping (draft-arias-noguchi-dnrd-objects-mapping).

Con la implementación del reglamento de privacidad (GDPR) en camino, puede ser insensato intentar avanzar con las partes técnicas, según Roger Carney (GoDaddy) y Richard Wilhelm (Network Solutions). Scott Hollenbeck pidió saber cuánto estaba en uso el estándar sobre el depósito de datos en un tercero por parte de los ccTLD y si es, por lo tanto, «global». De otro modo, propuso que el potencial documento fuera informativo en lugar de seguir el camino de los estándares.

Con respecto a la opción entre el camino informativo o de estándares, los autores de las propuestas usualmente piden el camino de los estándares en la reunión RegExt —destacando claramente el problema debatido durante la BoF sobre RFCPlus. Para conocer más detalles sobre la sesión del RDAP, vea las diapositivas del presidente y las minutas publicadas en una de las sesiones hasta ahora.

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

Grupos de Trabajo

DNS: ¿El «negocio de siempre» es suficiente?

Con el avance del DoH y la presión sobre la comunidad DNS proveniente de sus colegas Web, uno puede preguntarse si el WG del DNS terminará teniendo un debate fundamental sobre el futuro del DNS en términos más generales.

¿Something(CNAME)@APEX?

Según algunos, las reuniones conjuntas de las comunidades DNS y Web están en demanda urgente debido a desarrollos como el DNS sobre HTTPS, el DoH Digest, y también SRV en HTTP (quienes se reunieron en una BoF de bar – documentada aquí). La copresidente de DNSOP Suzanne Woolf dejó en claro que los presidentes consideraron que este trabajo estaba fuera del alcance del WG de DNSOP.

Aun así, la presión sobre el DNS proveniente de la Web fue evidente durante la reunión DNSOP en el debate sobre something@Apex. El copresidente del WG, Tim Wicinski, instó a que la comunidad DNSOP idee algún tipo de solución para permitir una resolución como CNAME (como la redirección de example.com a www.example.com). Wicinski señaló que un número de proveedores de servicios en la nube la tenían, aunque fueran soluciones propietarias temporales. Por ejemplo, Amazon la estaba ofreciendo, pero debido a que infringe estándares existentes, solo funciona cuando conocen el target (porque se encuentra en la base de datos de su propio cliente).

Aunque Wicinski solo pidió una solución que también permitiera a los operadores pequeños hacerlo de una manera que no infrinja los estándares (y no solo dejarla como un truco para los grandes), hubo una gran resistencia sobre qué problema sería resuelto. Como se debatió en la reunión paralela, el SRV sería una solución más limpia, a pesar de tener algunos problemas (casos de borde, por ejemplo), según señaló Stephane Bortzmayer. Fue un poco como resolver un problema que tenía otro problema, según dijeron Wes Hardacker y Joel Jaeggli.

CNAME + DNAME @ PARENT Results

DNSSEC Validation Enabled	No QNAME Minimization	Relaxed QNAME Minimization	Strict QNAME Minimization
BIND 9.11.4	OK!	N/A	N/A
BIND 9.12.2	OK!	N/A	N/A
BIND 9.13.2	OK!	OK!	OK!
PDNS Recursor 4.1.3	DNAME fails [2]	N/A	N/A
Unbound 1.7.3	OK!	OK!	OK!
Knot Resolver 2.4.0	N/A	Mixed [1]	N/A
Google Public DNS	OK!	N/A	N/A
Verisign Public DNS	OK!	N/A	N/A
Quad 9	DNAME fails [2]	N/A	N/A
Cloudflare 1.1.1.1	N/A	Mixed [1]	N/A

1. DNAME returns SERVFAIL *AND* Correct Resource Records
2. PowerDNS 4.2 has some DNAME fixes in the roadmap

Hubo experimentos que pusieron ya sea CNAME o CNAME más DNAME juntos en el Apex durante la Hackaton, llevados a cabo por Willem Torop (NLnet Labs) y Ondrej Sury (ISC). Actualmente, según

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

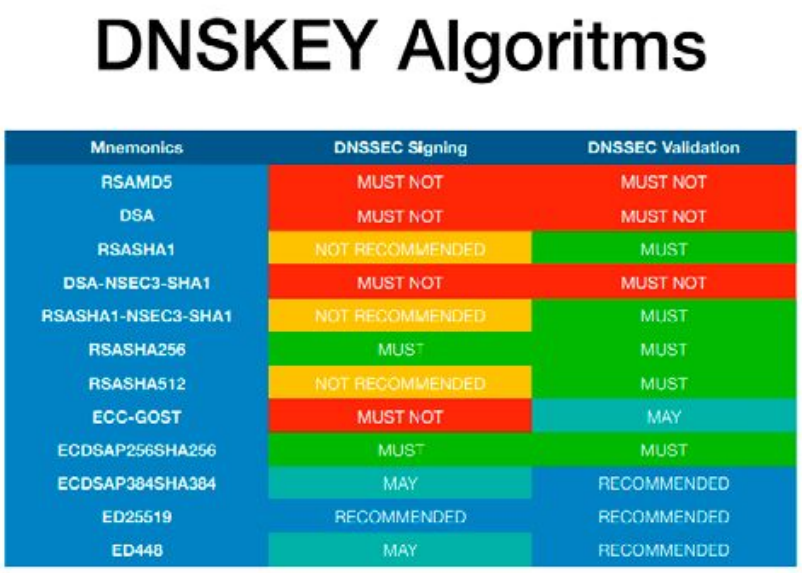
la RFC 1034, CNAME@Apex no está permitido: no permite tener CNAME RR a la par de otros datos, y funciona deficientemente. Sin embargo, la versión CNAME más DNAME funcionaba mejor (vea los resultados en el gráfico). Puede ver el antiguo *draft* de Sury sobre esta versión aquí.

Algunos se quejaron de que la gente del DNS no se había movido durante los últimos 20 años y que necesitaba un empujón. Otra reunión en Bangkok puede suceder a una reunión interina que Wicinski dijo que organizaría.

¡Cómanse esas cookies (del DNS)!

Otro tema controvertido en el debate en DNSOP fueron las cookies del DNS. Ondrej Sury y Willem Torop propusieron armonizar la implementación de las cookies mediante un documento RFC que estandarice el cifrado de las cookies y otros detalles operacionales. Actualmente, las discrepancias de proveedor múltiple y de mismo servidor resultarían en problemas con las diferentes versiones de las cookies del DNS que estén siendo utilizadas. Hasta grandes servidores como K-Root rotarían entre varias implementaciones para las cookies, también debido a las situaciones *anycast*. La propuesta de Sury y Torop es hacer obligatorias varias características para armonizar la producción y el consumo de cookies. Esto suscitó pedidos para ya no utilizar cookies, y más drásticamente, para «¡matar las cookies, y usar TCP (para un transporte con estado)!», según Olafur Gudmundson, de Cloudflare. Sin embargo, muchos expertos recalcaron que, siempre y cuando el UDP fuera una opción, debía estar asegurado y que las cookies eran una opción estandarizada en la RFC 7873.

Por el momento, el WG del DNS todavía tiene bastantes documentos en su agenda. La actualización del cifrado para las claves y validación de DNSSEC es relativamente no controvertida (vea el gráfico).



Varios de los *drafts* que llegaron a la mesa del IESG (pasando por la última llamada del WG) incluyen:

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

- draft-ietf-dnsop-kskroll-sentinel
- draft-ietf-dnsop-terminology-bis
- draft-ietf-dnsop-attrleaf
- draft-ietf-dnsop-attrleaf-fix
- draft-ietf-dnsop-isp-ip6rdns

Uno de los documentos debatidos durante mucho tiempo, el 5011 sobre las consideraciones de seguridad de implementación de clave, todavía espera el apoyo o la objeción del WG para proseguir. Durante la reunión en Montreal, Mike St. Johns del IESG dijo que, aunque tiene sentido en su forma actual, el documento es más dañino que útil. El autor, Wes Hardacker, dijo que no pretendía volver atrás para hacer más cambios: le pidió al WG que decidiera cómo proceder.

Nuevos trabajos en la mesa del WG del DNS que parecen seguir adelante son una solución de proveedor múltiple para DNSSEC (el WG adoptó el documento) y potencialmente una manera de reportar que un padre solo delega y no firma registros de su hijo. Según el autor Paul Wouters (Apache), esto daría transparencia a los potenciales intentos de los padres de firmar registros de las zonas de los hijos.

Wouters también presentó una propuesta para evitar los posibles ataques de degradación a la cadena de extensiones DNSSEC. Con las claves en el DNS (Autenticación DANE de un servidor TLS), existió la necesidad de implementar seguridades adicionales contra los ataques de degradación. Wouters dijo que el WG de TLS y el WG del DNS podrían considerar las siguientes respuestas:

- No actuar.
- Reparar todo en la nueva extensión de TLS.
- Dos *zero bytes* en esta RFC, especificar una semántica *non-zero* en una actualización RFC separada.
- Extensión TLS con un TTL pin de dos bytes (en horas).
- Campo reservado (vacío por defecto) de longitud variable (0..255) en esta RFC, sintaxis y semántica en una actualización RFC separada.
- Bloqueo de extensión anidada (como la nueva extensión TLS, pero más complicada aún).

Para más información, vea las minutas exhaustivas aquí. El WG de DNSOP tiene un nuevo y tercer copresidente: Benno Overeinder, de NLNet Labs, para ayudar con el volumen del trabajo.

WG de DPRIVE: Carta constitutiva reformulada, el autoritativo todavía no alcanzado

El WG de DPRIVE ha reformulado su carta constitutiva desde el IETF101 y, según la nueva carta, tiene el siguiente alcance:

1. Proveer confidencialidad a las transacciones DNS entre Resolutores Iterativos y Servidores Autoritativos.
2. Medir la eficacia de la preservación de la privacidad de cara a ataques de monitoreo ubicuos.

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

3. Definir las consideraciones operacionales, políticas y de seguridad para los operadores del DNS que ofrecen servicios de privacidad del DNS. Algunos de los resultados de este WG pueden ser experimentales.

En Montreal no se debatió —como se había planificado— el tema de la extensión del DNS sobre TLS desde el resolutor *stub* al autoritativo considerada como el siguiente paso inmediato tras asegurar la parte del *stub* al resolutor. En cambio, debido a limitaciones de tiempo en Montreal, el copresidente Tim Wicinski anunció una reunión interina más adelante en el verano, que debatirá cómo proceder para asegurar las ramas más bajas del árbol del DNS. El documento de Stephane Bortzmeyer ha estado dando vueltas desde hace tiempo, pero no ha suscitado mucho debate.

El desarrollo paralelo del DoH podría ciertamente haber resultado en la desaceleración de los desarrollos del DNS sobre TLS. Las cifras del despliegue del DNS sobre TLS tras cuatro años todavía parecen crecer muy lentamente —a pesar de la disponibilidad de la opción en la mayor parte del *software* de código abierto del DNS.

Brian Haberman, copresidente del WG de DPRIVE, informó, a partir de una campaña de medición de RIPE Atlas que de 3.659 servidores DNS únicos consultados (en total, 40.841 consultas), 61 servidores DNS respondieron sobre TLS. Solamente el 1,67 por ciento de los servidores permite el DNS sobre TLS. «Las mediciones de algunos servidores que permiten el DNS sobre TLS fallaron debido a la disparidad de capacidad de TLS», añadió también Haberman.

El *draft* de coautoría de Sara Dickinson por un documento de mejores prácticas (BCP) sobre una guía operacional para los servicios de privacidad del DNS aborda el tercer punto de la nueva carta constitutiva («definir las consideraciones operacionales, políticas y de seguridad para los operadores del DNS que ofrecen servicios de privacidad del DNS»). El documento brinda un panorama general sobre las variadas opciones que ahora están disponibles para el transporte cifrado (DNS sobre TLS, DNS sobre HTTPS), debate las distintas características y brinda asistencia a operadores en la redacción de un documento sobre sus prácticas operacionales con respecto a la privacidad, una Declaración sobre Políticas de Privacidad y Prácticas del DNS (DPPS, por sus siglas en inglés). La DPPS puede publicarse para permitir que los clientes evalúen las políticas de privacidad del operador del DNS. La opinión en la sala favoreció conservar las dos partes (características de privacidad y la DPPS) en un documento.

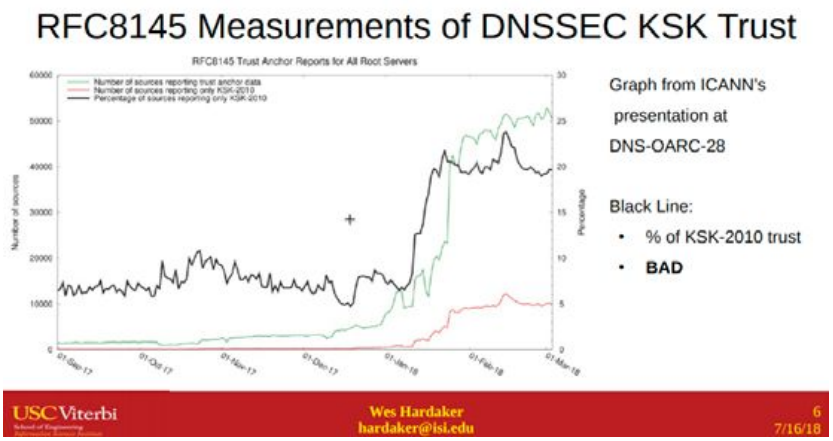
El BCP también enumera las políticas de privacidad de los operadores del DNS más importantes (Quad9, Cloudflare, Google y OpenDNS) y apunta a una mesa llena que incluya a los operadores pequeños aquí.

MAPRG: Problemas de implementación de DNSSEC y otras mediciones del DNS

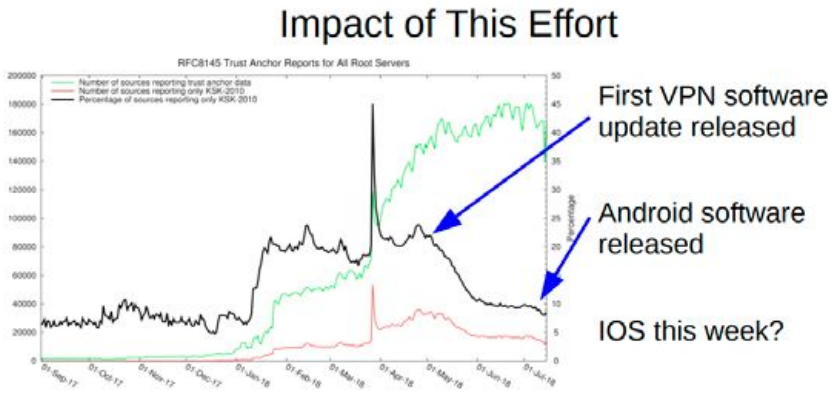
El DNS también fue un tema central en la sesión de Montreal en el Grupo de Investigación de Mediciones y Análisis para los Protocolos (MAPRG, por sus siglas en inglés). Con el ancla de confianza señalizando con RFC 8145, los expertos están tratando de entender la lenta tasa de implementación de la KSK 2017. El otoño pasado, la lenta tasa de implementación y la falta de perspectiva en cuanto a la situación hizo que ICANN detuviera la implementación planificada de

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

la nueva clave. Wes Hardacker presentó un estudio de caso que ilustra el problema de un operador VPN.



Al analizar la cantidad de fuentes que señalaban que solo tenían la antigua KSK a comienzos de 2018, Hardacker y sus coautores descubrieron que, en lugar de disminuir, el número había estado aumentando a comienzos del año en el servidor raíz B-Root. Observando fuentes relevantes, Hardacker descubrió que el 63 por ciento de las fuentes enviaron solo unas pocas (una o dos) consultas al mes. Un cuarto de las consultas analizadas fueron a un proveedor VPN. Al contactar al proveedor correspondiente, serán lanzadas actualizaciones Android/Software de sistemas operativos para mitigar el problema. Hardacker concluyó que los cambios inmediatos eran difíciles (la implementación de la KSK está establecida para el 11 de octubre de 2018) y que el software debería incluir actualizaciones de clave DNSSEC automáticas, antes que nada.



DMAP: Mediciones del DNS más fáciles y unificadas

Trabajos relacionados con el DNS incluyeron la presentación de una nueva herramienta para mapear las propiedades del DNS. El DMAP, que mapea el ecosistema de los nombres de dominio, automatiza las mediciones de cinco protocolos: HTTP, HTTPs, DNS, TLS y SMTP.

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

Permite una vista unificada mediante una interfaz SQL. Todos pueden probar y usar la herramienta realizada por SIDN aquí.

Cacheo y efectos de reintento durante los ataques DDoS

Un estudio sobre el cacheo y los reintentos cuantificó la cantidad de consultas respondidas durante los ataques DDoS bajo diferentes TTL. El estudio concluye que, juntos, el cacheo y los reintentos permiten que hasta la mitad de los clientes tolere ataques DDoS que resultan en una pérdida de consulta del 90%. Casi todos los clientes pueden tolerar ataques que resultan en una pérdida de paquete del 50%. La latencia remanente se incrementa para los clientes durante los ataques. Según los resultados para los servidores, los reintentos multiplican el tráfico normal hasta 8 veces.

ANRW: El DNS, certificados filtrados y aumento del nivel del mar

Por primera vez, el Taller de Investigación de Redes Aplicadas (ANRW, por sus siglas en inglés) tuvo lugar en el mismo momento que la reunión IETF habitual, en lugar de una semana antes. Tanto los científicos como los participantes del IETF recibieron de buena manera el calendario, ya que permitió que las dos comunidades se reunieran.

La copresidente del ANRW, Sharon Goldberg, pidió que a la comunidad académica no espere que sus ideas y propuestas sean tomadas en consideración por los ingenieros y se conviertan en RFC. Goldberg guió brevemente a quienes estaban interesados sobre qué pasos seguir para que sus *drafts* sean aprobados por el IETF. Las sesiones significativas cubrieron los temas de TLS, enrutamiento, infraestructura y comunicación anónima.

El DNS fue el tema de una de las charlas invitadas en la que Mark Allman (del Instituto Internacional de Informática de la Universidad de Berkeley) presentó cifras sobre la progresiva concentración en el DNS. Al abordar la robustez, que consiste según la RFC 1034 en tener dos servidores de nombres autoritativos por cada SLD y distribuirlos geográficamente según la RFC 2184, Allman descubrió que un creciente número de SLD sí cumplían con los estándares mínimos establecidos en las RFC. Profundizando un poco más, sin embargo, también pudo medir que el 20 por ciento de todos los SLD son resueltos a partir de solamente 19 redes (el puesto 1 y el 4 en la tabla pertenecen a Cloudflare, por ejemplo).

Rank	Full SLDs	Partial SLDs	/24s	Same Last Hop
1	71,472	3,066	2	✓
2	69,637	328	2	
3	15,421	17	2	✓
4	13,044	3,727	2	✓
5	8,347	3	2	
6	6,111	631	2	✓
7	5,568	375	3	✗
8	5,076	69	2	
9	4,788	648	2	
10	4,611	4,820	4	
	204,075	–	23	–

Table 2: Information about the top ten SLD groups based on /24 address prefix.

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

Allman lo llamó un «hábito no saludable», como mínimo. Estuvo de acuerdo en que hace falta investigar más profundamente la concentración de la infraestructura del DNS además de la tendencia hacia el uso de solo algunos grandes proveedores de servicios en la nube y grandes hospedajes. Dijo que el uso de *anycast* regionalizaría, pero no resolvería necesariamente por completo el problema de la robustez (ser capaz de encontrar siempre un servidor autoritativo para un nombre consultado).

Allman recibió una invitación por parte de Ondry Sury (ISC) para la próxima reunión DNSOARC en Ámsterdam en octubre (a la par de la reunión RIPE).

TLS 1.2 y certificados de clientes filtrados

Otras charlas sumamente interesantes tocaron el tema de la filtración de datos mediante el TLS 1.2 en relación con los certificados de los clientes. Los certificados no están cifrados en el TLS 1.2. Debido a que los certificados de los clientes contienen mucha información, los usuarios podrían ser rastreados individualmente, según descubrieron los investigadores de la Universidad Técnica de Múnich. En su *paper*, demuestran cómo el servicio de notificaciones push de Apple permitía este tipo de rastreo con cada autenticación para una nueva sesión de TLS 1.2 que brinda un marcador del paradero del usuario. Para cuando los investigadores la contactaron, Apple ya había cerrado la filtración. Sin embargo, los certificados de clientes también se usan en otros lugares, por ejemplo, en las comunicaciones móviles y las VPN. Mientras utilice el TLS 1.2, debería evitarse el uso de la autenticación de certificado del cliente, según el autor Quirin Scheitle.

Otra charla presentó las predicciones sobre el impacto del aumento del nivel del mar debido al cambio climático en la infraestructura del cableado en EE. UU. En base a las proyecciones de las incursiones sobre el nivel del mar de la Administración Nacional Oceánica y Atmosférica (NOAA, por sus siglas en inglés) y los datos del despliegue de la infraestructura de Internet en el Internet Atlas, los investigadores de la Universidad de Óregon descubrieron que 4.067 millas de conducto de fibra óptica estarán bajo el agua y 1.101 nodos (por ejemplo, puntos de presencia y centros de colocación) estarán rodeados de agua en los próximos 15 años. Las regiones con un riesgo especial son las áreas metropolitanas de Seattle, Nueva York, y Miami.

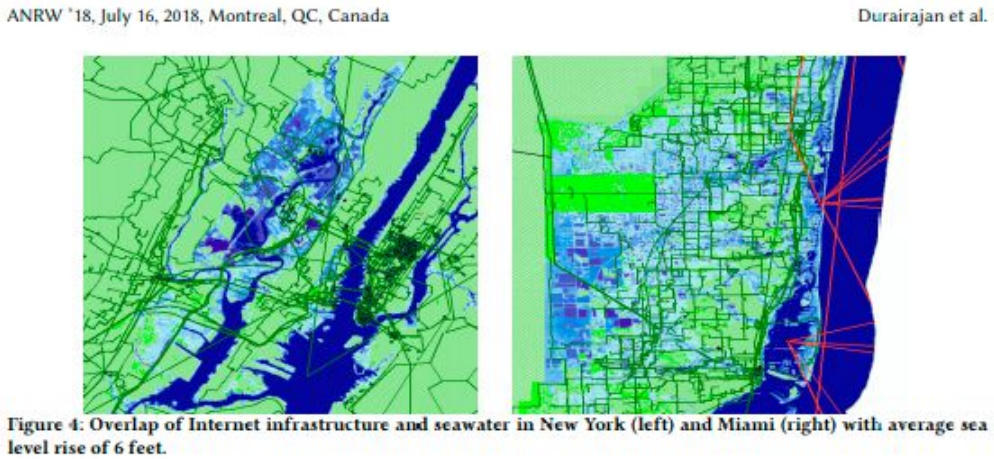


Figure 4: Overlap of Internet infrastructure and seawater in New York (left) and Miami (right) with average sea level rise of 6 feet.

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

De las infraestructuras de proveedores de servicios individuales, las que están en el riesgo más alto son Level3, Inteliquent, y AT&T. Los investigadores instaron al desarrollo de estrategias de mitigación, por ejemplo, el despliegue de infraestructuras alternativas. No consideraron otras partes del mundo.

TLS: Cifrar el SNI

El WG de TLS adoptó un documento que apunta al cifrado del Identificador del Nombre del Servidor (SNI, por sus siglas en inglés) durante la reunión en Montreal. La falta de oposición fue una sorpresa, ya que varios expertos habían expresado sus objeciones en la lista de correos antes de la reunión del IETF. El SNI es uno de los puntos que quedan sobre los metadatos aún disponibles con la mayoría de los *handshakes* cifrados en el TLS 1.3.

El TLS 1.3 cifra muchos puntos de datos, incluyendo el certificado. El SNI se creó originalmente para identificar el receptor de un paquete, ya que debido a la nube y las CDN, las direcciones IP se comparten regularmente. Prácticamente, los SNI ofrecían un reporte que permitía la diferenciación por calidad de servicio y la censura. El WG llevaba tiempo debatiendo el filtrado mediante los SNI y la posible mitigación. Hasta ese momento no se había buscado una solución independiente para el cifrado de los SNI, porque los expertos temían que, debido a la complejidad, habría pocos ejecutantes, haciendo que sobresalgan. Los autores de Apple y Mozilla ahora esperan que las fuentes privadas se escondan en redes y servidores de aplicaciones más grandes. Si estos cambiaran a ESNI, entonces esto solo apuntaría al proveedor de la aplicación, el servidor en la nube o la CDN.

Técnicamente, el proveedor publicará la parte pública de una clave, posiblemente en el DNS (como txt o registro de recurso). Las DNSSEC pueden brindar autenticación. El proveedor finalmente descifra con la clave privada y envía los paquetes al receptor deseado. Según Eric Rescorla, esto sería bastante directo. Los enrutadores domésticos que bloquean el tráfico cifrado continúan siendo una posible fuente de conexiones fallidas.

Varios representantes de empresas rechazaron la propuesta en la lista de correos una vez que se publicó; algunos advirtieron que el equilibrio entre la privacidad y la manejabilidad de las redes se había movido mucho en la dirección del primero. La exdirectora de Área de Seguridad Kathleen Moriarty (Dell) se quejó de que, hasta el momento, el WG había expresado que no llegaría al punto de cifrar el SNI. La declaración de Moriarty fue rechazada por Rescorla y otros que apuntaron al *draft* previo.

No queda claro si las preocupaciones del ESNI se originan en los mismos grupos que piden claves estáticas en el TLS 1.3 para permitir mejor manejabilidad del centro de datos. Es interesante, sin embargo, que un representante del Centro de Ciberseguridad Nacional Británico pidió algún lugar en el IETF para debatir los efectos colaterales de los protocolos cifrados para la defensa cibernética y la aplicación de la ley. Durante el IETF en Londres, el Centro de Ciberseguridad Nacional había opinado fuertemente a favor de una clave estática en el TLS 1.3.

Otra preocupación está relacionada con la continua centralización. Con la solución ESNI contribuyendo al gran modelo de plataformas por oscuridad, la tendencia hacia la centralización y la concentración continúa.

La próxima reunión del IETF tendrá lugar en Bangkok del 3 al 9 de noviembre de 2018.

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