Informe de CENTR

IETF 106

Singapur, 16 - 22 de noviembre de 2019

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

Contenidos

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

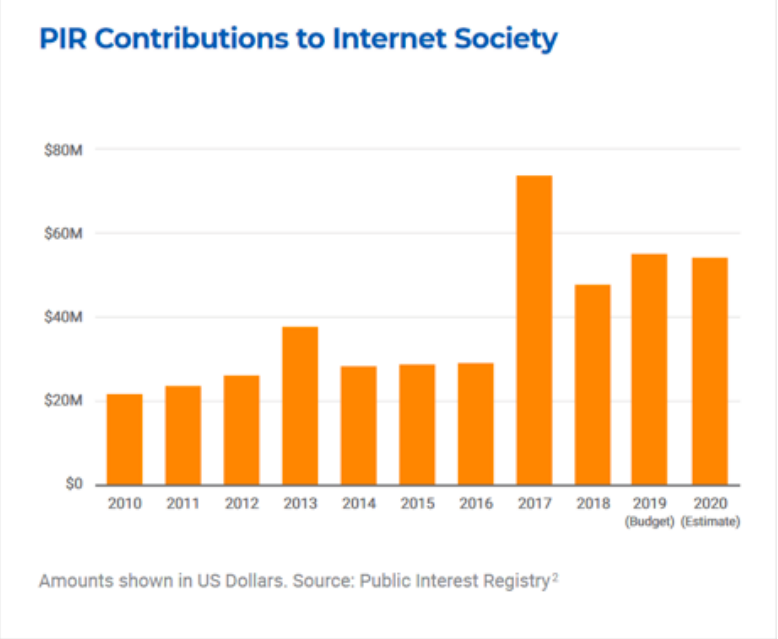
Aspectos destacados

La batalla por el PIR

Ethos Capital ha acordado comprar el Public Interest Registry (PIR) de la Internet Society (ISOC) con todos sus activos. La noticia se anunció el 13 de noviembre de 2019, apenas tres días antes del comienzo de la reunión IETF en Singapur. Desde afuera, puede parecer una transacción de negocios normal, pero algunas partes de la comunidad de Internet se pusieron en alerta y, consecuentemente, se comunicaron con ISOC para hacer preguntas.

¿Vender una fuente de ingresos?

La pregunta más importante tuvo que ver con la motivación para la venta de lo que se puede considerar como la fuente de ingresos de ISOC durante los últimos 15 años. En 2018, se concluyó que el PIR solo podría generar 43 millones de dólares para ISOC, obtenidos del negocio del registro con .org, el reciente .ngo y la versión .org en alfabeto cirílico. En 2017, durante una ola excepcional de registraciones de dominios, ISOC recibió casi el doble de ese monto: aproximadamente 80 millones de dólares estadounidenses. Dejando de lado ese año, que fue un caso particular y se originó a partir del acaparamiento de dominios, el PIR aseguró, de igual manera, un ingreso relativamente estable a lo largo de los años, lo que permitió que la organización llegue a estar conformada por 50 personas, habiendo empezado solo con dos. La pregunta es, entonces, ¿la organización vendió su fuente de ingresos?



El CEO de ISOC, Andrew Sullivan, explicó que uno de los motivos principales fue la diversificación de las fuentes de financiación de la organización. Al depender solo de un sector —el negocio de los nombres de dominios—, la organización está más sujeta a las fluctuaciones

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

de esta industria. Con el monto recibido por la venta, ISOC sería libre de hacer inversiones más diversas, según Sullivan. El CEO reconoció que, para igualar el ingreso actual, la venta debió realizarse por una gran cantidad de dinero.

En paralelo, señaló que las grandes y medianas fundaciones habitualmente podían ganar un 8 o 9 por ciento de sus donaciones. Sullivan comentó que fue necesario contar con los asesores adecuados para tomar buenas decisiones de inversión, y agregó que, actualmente, solo podía decir que la Junta Directiva de ISOC había cumplido con su trabajo. El monto real que pagará Ethos no será revelado por ahora porque, según Sullivan, Ethos Capital solicitó que así fuera. Sin embargo, el monto se hará público apenas ISOC publique su propio informe anual.

Los cálculos sobre cuánto debe recaudar ISOC a partir de la transacción para igualar su flujo de ingresos actual varían: algunos consideran que un monto entre 500 y 600 millones de dólares será suficiente, mientras que otros afirman que se necesitan mil millones.

Secretismo

El nivel de secretismo que envuelve la transacción fue otra de las cuestiones que plantearon al menos algunos observadores, miembros y capítulos de ISOC. La Junta Directiva de ISOC, el PIR y Ethos Capital lograron mantener ocultas las negociaciones. Si bien este pudo haber sido un pedido del nuevo inversor, esto ha creado sospechas e hizo que la promesa de que "Tras el cierre de las transacciones, el PIR seguirá cumpliendo los más altos estándares de transparencia pública, rendición de cuentas y rendimiento social acordes a su antigua misión y propósito, y considerará obtener la certificación de Corporación B" suene, como mínimo, un tanto vacía.

¿Quién es Ethos Capital?

Muchos también preguntaron quién era Ethos Capital, ya que no es un nombre reconocido en la industria de los dominios. De hecho, la empresa parece nueva, el sitio web carece de los detalles que se le exigen a una organización transparente y, en algunos países, carece incluso de una presencia web como empresa legítima. Su vínculo con la industria de los nombres de dominios radica en que su fundador, Erik Brooks, que en su momento estaba trabajando para Abry Partners, organizó la adquisición de Donuts por parte de Abry. Mediante ese negocio, en el que el exdirector ejecutivo de ICANN, Fadi Chehade, actuó como asesor, Abry se puso en contacto con Chehade y ICANN. Solo hay otra persona que se menciona en el sitio web ethoscapital.org: un exempleado de ICANN. De hecho, Chehade registró el nombre de dominio ethoscapital.org en mayo de 2019, en la época en que ICANN anunció que aumentarían los precios máximos de .org (junto con otros TLD).

Debido a los fuertes comentarios y una serie de artículos altamente críticos (por ejemplo, el artículo de Kieren McCarthy) tras la reunión directiva en Singapur, ISOC publicó una sección de preguntas frecuentes que abordan las principales preocupaciones de los capítulos y miembros de ISOC. Puede ver algunos ejemplos a continuación.

> "***¿Abry Partners participa en esta transacción?***

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

Abry Partners no forma parte de esta transacción. Abry Partners es una empresa de capital privado para la que Erik Brooks trabajó durante 20 años, antes de dejarla para establecer Ethos Capital.

¿Fadi Chehade participa en esta transacción?

La empresa de Fadi Chehade, Chehade & Company, es una consultora de Ethos. Chehade & Company es una empresa consultora que tiene clientes en los sectores de tecnología, educación y el sector creativo.

Chehade es miembro de la Junta de Sentry Data Systems and Interactions LLC y es miembro de la junta consultiva del Centro para la Cuarta Revolución Industrial del Foro Económico Mundial. Anteriormente, fue presidente y CEO de ICANN, miembro del Panel de Alto Nivel del Secretario General de Naciones Unidas sobre Cooperación Digital y asesor sénior del presidente ejecutivo del Foro Económico Mundial".

¿Qué significa esto para la comunidad org y el IETF?

Para el IETF, fue importante una de las preguntas del trato: ¿ISOC seguirá siendo espónsor del IETF? ¿O será tarea de la nueva organización ser espónsor del IETF? A pesar del plan del IETF de volverse más independiente, organizativa y financieramente, ISOC sigue siendo una fuente importante para su financiamiento o, por lo menos, una red de contención para el IETF.

Sullivan aclaró que el financiamiento del IETF no provendría del "Fondo de Habilitación de Ethos Capital para la Comunidad para apoyar el financiamiento de iniciativas actuales y adicionales llevadas a cabo por organizaciones de Internet importantes" (una de las tres obligaciones autoimpuestas que Ethos anunció en un posteo de blog con ISOC). Sullivan remarcó que el financiamiento del IETF seguirá proviniendo de ISOC.

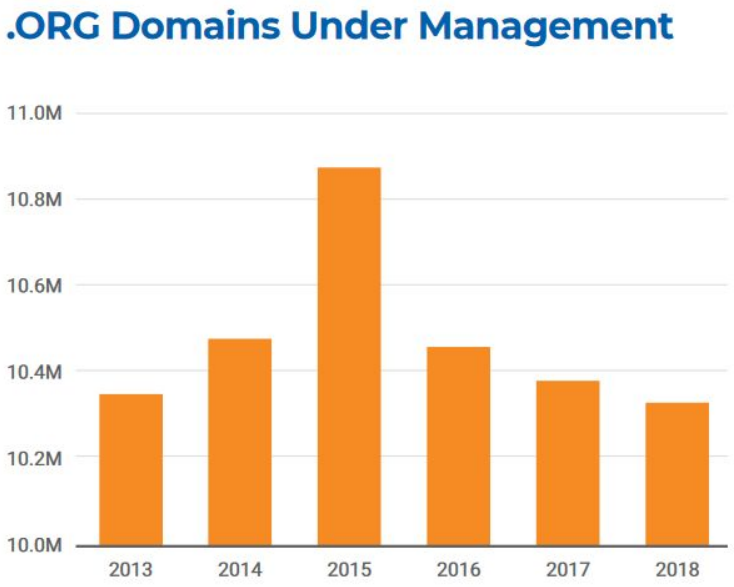
Tanto los opositores como los defensores están de acuerdo en un aspecto: los registrantes de .org deben prever que los precios subirán con Ethos, especialmente si compró el PIR por una gran suma de dinero. Nuevamente, hay discrepancias sobre cuánto afectará a las personas y a las organizaciones sin fines de lucro con más de un dominio .org. Los defensores afirman que solo los acaparadores serán afectados, pero algunos creen que las ONG en países en desarrollo o países menos desarrollados también sufrirán el cambio.

¿Los reguladores aprobarán la transacción?

En total, hay tres "autoridades" diferentes que deben aprobar el trato firmado por las partes: ICANN, el Procurador Estatal de Pensilvania (donde está constituido el PIR) y el Fondo para Huérfanos y Viudas. El Procurador Estatal debe aprobarlo porque, mediante este trato, el PIR se convierte en una empresa privada con fines de lucro.

Algunos críticos esperan que estos pasos regulatorios detengan el trato: un grupo emitió una petición en change.org que cobró impulso lentamente, con casi 420 firmas luego de una semana. La reacción de ICANN ante las solicitudes de prensa fue simplemente reconocer que había recibido las solicitudes y que estaba revisando los detalles.

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



Source: Public Interest Registry[3]

Un nuevo DNS: ADNS, ODNS

La búsqueda de la solución a la disputa del DoH continúa. Ni Google ni Cloudflare ni Mozilla presentaron las propuestas más nuevas para arreglar la implementación del DoH. En cambio, un grupo de ingenieros de Apple (y una nueva y rápida "adquisición", Patrick McManus, previamente de Mozilla) presentó el "Adaptive DNS" (ADNS). Según Tommy Pauly (Apple), el objetivo expreso de la nueva especificación propuesta es mejorar la privacidad sin contar con un resolutor público arreglado.

La arquitectura del ADNS

En lugar de enviar todas las consultas DNS a un resolutor fijo —como en la implementación de DoH de Mozilla— el ADNS revisa una lista de opciones para lograr la resolución de nombres. Si bien no exige la intervención del usuario para elegir una opción, el ADNS depende de una serie de elementos nuevos, desarrollados en otros Grupos de Trabajo (WG). Los elementos necesarios de la arquitectura del ADNS son los siguientes:

1. Un registro DNS que indique un servidor DoH designado asociado a un nombre (*draft* en DNSOP).

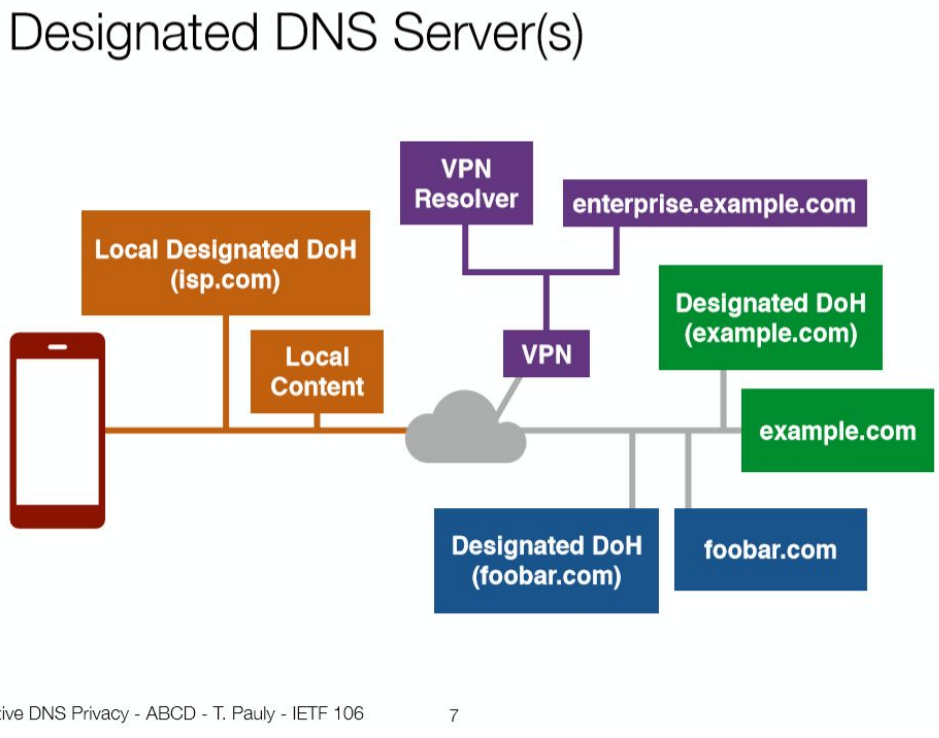
2. Una extensión al DoH que permita que las direcciones IP del cliente sean desvinculadas de las consultas mediante un proxy (*draft* en DPRIVE: I-D.pauly-dprive-oblivious-doh).

3. Un servidor DoH que responda directamente las consultas y soporte la función proxy.

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

4. Normas de comportamiento del cliente sobre cómo resolver nombres utilizando una combinación de resolutores DoH designados, consultas que pasaron por un proxy, y resolutores locales.

El concepto básico del ADNS es permitir que las solicitudes sean manejadas "flexiblemente" de manera local (según las políticas correspondientes, ya sea en base al filtrado o brindando servidores de nombre internos) o con un servidor DoH "designado" responsable de un dominio consultado que el cliente sabe que ofrece resolución DoH para el dominio correspondiente.



Un nuevo tipo de registro para el servidor DoH designado

Para el *bootstrapping*, un cliente debe tener conocimiento de al menos uno o dos dominios con sus propios resolutores DoH, que deben ser consultados sobre el DNS clásico o los resolutores DoH conocidos se convierten en la configuración por defecto. Más adelante, el *draft* incluye como opciones posibles las listas blancas o el protocolo de configuración de *host* dinámico (DHCP).

Los servidores DoH de una zona determinada señalan su rol de resolutor para el dominio mediante nuevos registros de enlace de servicio: HTTPSSVC, SVCP. Según las novedades del DNSOP, los registros HTTPSSVC/SVCP serán consultados a la par de los registros A/AAAA. El WG de DNS presentó un *draft* especial para este nuevo registro.

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

Una vez establecida la relación, el servidor designado no solo brinda las respuestas para la zona correspondiente, sino que también actúa como proxy para resolver dominios por fuera de su zona para el cliente que hace la consulta.

Oblivious DNS (ODNS)

Para contenido altamente sensible que un usuario desee ocultar de todos excepto del servidor autoritativo, se propone otro tipo de resolución de consultas. Bajo el nombre de "Oblivious DNS" (¿ODNS?), el cliente envía solicitudes cifradas a un "proxy desentendido" (*oblivious proxy*) que no las descifra y responde, sino que las envía a otro servidor, el "target desentendido" (*oblivious target*), que las descifra y lleva a cabo la resolución. Este concepto, propuesto como una extensión al DoH y descripto en un *draft* por separado, divide el conocimiento acerca de los datos de la consulta y la dirección IP. Un ataque conocido sucede cuando un "oblivious proxy" y un "oblivious target" colisionan.

Qué resolutor usar

Debido a que ahora existe una serie de diferentes opciones de resolución, el *draft* de ADNS enumera claramente en qué orden deben usarse los diferentes modos de resolución, según el nombre de *host* específico:

1. Resolutor Directo Exclusivo (resolutor provisto por VPN con normas de dominio para el nombre de *host* resuelto). Si la resolución falla, la conexión también fallará.

2. Resolutor Directo, como un enrutador local, con normas de dominio conocidas por ser autoritativas para el dominio que contiene el nombre del *host*. Si la resolución falla, la conexión intenta con la siguiente configuración de resolutor en base a la lista.

3. El Servidor DoH Designado más específico que se haya incluido en la lista blanca. Por ejemplo, si tenemos dos Servidores DoH Designados, uno para "foo.example.com" y otro para "example.com", los clientes que se conecten a "bar.foo.example.com" deberían usar el primero. (Los clientes sensibles en cuanto a privacidad no deberían continuar con el siguiente).

4. Las consultas del Oblivious DoH que usen múltiples Servidores DoH. Si la resolución falla, las conexiones sensibles en cuanto a privacidad no deberían resolver.

5. El Resolutor Directo predeterminado, generalmente el resolutor provisto por el enrutador local, se usa como último recurso para cualquier conexión que no sea explícita.

¿Por qué DoH y no DoT?

Durante su presentación, Pauly respondió lo que, según él, eran las preguntas más frecuentes hasta el momento. Explicó que la elección del DoH en lugar del DoT surgió del potencial de la reutilización de la conexión, la opción de multiplexación y, además, una migración más sencilla al nuevo protocolo de transporte: QUIC. Sin embargo, Pauly señaló que el ADNS también podría designar servidores DoT. El segundo problema era la expectativa de que los resolutores designados debían estar firmados por DNSSEC; de lo contrario, los atacantes podrían dirigir el

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

tráfico hacia ellos mismos. Esto podría representar una barrera de entrada, dada la tasa de adopción.

Reacción del WG

Si bien hubo comentarios positivos durante la BoF de ABCD (seguimiento de DoH) y durante la sesión de DPRIVE sobre el intento de crear una implementación de DoH descentralizada, algunos observadores plantearon preguntas un tanto fundamentales. Alex Mayrhofer (nic.at) remarcó que el ADNS crearía un mundo completamente nuevo respecto de cómo se trata el DNS, especialmente al levantar la barrera entre el resolutor y el servidor DNS autoritativo, ya que los servidores designados DoH serían autoritativos para un dominio/algunos dominios al igual que al resolver otros. Ben Schwartz (Google), autor del *draft* de SVCP, habló de un "resolutor de cambio de modos".

Mayrhofer, en cambio, lo llamó "el archivo hosts.txt para el siglo XXI". Hosts.txt es la lista de *hosts* en Internet que se manejaba manualmente antes de que se estandarizara el DNS en 1983/84.

Stephen Farrell (IAB, y exdirector del Área de Seguridad) recibió con satisfacción la propuesta, pero advirtió contra las actitudes demasiado optimistas respecto del despliegue de DNSSEC. Con respecto a la privacidad, Vittorio Bertola (OpenNet) opinó que, si bien la descentralización era un buen avance, la distribución/propagación de los datos del DNS a diferentes partes no era un progreso. Se puede esperar que DPRIVE asuma este trabajo como una tarea del WG, junto con el *draft* de "oblivious" —que, según algunos, se acerca conceptualmente a TOR. Si se implementa ampliamente, la propuesta podría cambiar la cara del DNS significativamente.

ABCD: una BoF fallida

Pauly también presentó su *draft* sobre la muy esperada BoF de ABCD, un seguimiento de las disputas sobre la implementación de DoH de Mozilla. La BoF no logró acordar la formación de un grupo de trabajo en Singapur, debido a un texto de acta constitutiva artificialmente inflado, del que son responsables, principalmente, los presidentes de la BoF.

La propuesta canario de Mozilla y más

ABCD consideró las presentaciones sobre la propuesta de descubrimiento de Pauly como un mecanismo posible para evitar forzar el uso de un mecanismo de resolución DNS para todos los que usen una determinada aplicación.

Andy Grover presentó la solución rápida de Mozilla para este problema con la propuesta de dominio "canario". Al utilizar la prueba de dominio canario, la empresa del navegador verificará si los clientes han establecido algún tipo de mecanismo de control parental. Como un paso para hacer que el DoH sea el valor predeterminado, Firefox intentará resolver el dominio canario usando la configuración del DNS local. Si el dominio canario está bloqueado, Mozilla lo toma como una señal de que el software parental del DNS está funcionando y no procederá a establecer al DoH como predeterminado para el respectivo cliente.

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

Técnicamente, los operadores deben colocar el dominio canario . use-application-dns.net en su lista de bloqueo para permitir las respuestas de NXDomain o Servfail o para la devolución de un código NOERROR que viene sin registros A o AAAA. Grover dijo que la empresa no podía esperar para la estandarización, ya que necesitaba una solución rápida. Si bien no se explayó, la empresa está bajo escrutinio por parte de legisladores de EE. UU. y, claramente, ha estado bajo presiones para encontrar una solución. Además, Grover comunicó que Mozilla estaba muy interesada en estandarizar la solución, a fin de evitar múltiples soluciones canario para quienes potencialmente implementen el DoH. La respuesta de Mozilla ante las presiones políticas hizo que las personas cuestionen la motivación expresada con respecto al DoH en primer lugar. Mozilla había argumentado que proteger la red contra la censura era una de las motivaciones. La pregunta es cómo se puede evitar que los actores maliciosos (el estado/la red estatal) impidan el cifrado del tráfico DNS dada la opción de detenerlo mediante la solución canario.

Debate sobre la noción de "consenso total" en lugar del debate sobre el acta constitutiva de ABCD

Aunque la propuesta de Pauly encajaría perfectamente en el trabajo del WG de DPRIVE (y, aparentemente, terminará allí), la propuesta del dominio canario ciertamente no coincide con el acta constitutiva del WG de DPRIVE. Además, los presidentes de la BoF de ABCD enumeraron una serie de *drafts* adicionales sobre la configuración del cliente y sobre las consideraciones sistemáticas con respecto a los problemas de los operadores y de centralización con respecto al DoH:

2019: *drafts* sobre la configuración del cliente

- DNS Resolver Information Self-publication (adoptado en DNSOP)
- DNS Resolver Information: "DoH"
- DNS Resolver-Based Policy Detection Domain (presentado en DPRIVE y la BoF de ABCD)
- Adaptive DNS: Improving Privacy of Name Resolution (presentado en DPRIVE y la BoF de ABCD)
- A Bootstrapping Procedure to Discover and Authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers
- Selecting Resolvers from a Set of Distributed DNS Resolvers
- DNS over HTTP resolver announcement Using DHCP or Router Advertisements
- Indication of Local DNS Privacy Service During User Access
- Client DNS Filtering Profile Request

2019: *drafts* sobre consideraciones sistémicas relevantes

- DNS over HTTPS (DoH) Considerations for Operator Networks
- A privacy analysis on DoH deployment
- Centralised DNS over HTTPS (DoH) Implementation Issues and Risks
- Centralised Architectures in Internet Infrastructure

El debate sobre el acta constitutiva en Singapur, sin embargo, degeneró en un pleito sobre el texto que los copresidentes habían agregado al texto original, que era más ligero y específico. El concepto de "consenso total", en particular, generó mucho debate. Una sección agregada poco antes de la reunión IETF 106 enumeraba una serie de temas polémicos (privacidad y vigilancia

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

generalizada de los usuarios finales, detección y eliminación de *malware*, uso de registros de fuentes no confiables, cumplimiento de políticas y control de la configuración del resolutor *stub*, uso e impactos de grandes servicios de resolución recursiva), que fueron declarados como no temas, indicando que: "el grupo de trabajo no intentará resolver discrepancias sobre estos temas, y exigirá consenso total en todas las declaraciones sobre estas áreas".

Notable changes (1)

ORIGINAL	LATEST DRAFT
Specific initial areas of focus include: • Resolver discovery • Expression of resolver policy • Query routing in the presence of resolver choice	• Communicating configuration between the network, operating system, and applications • Discovery of resolvers and their capabilities and behaviors • Query routing in a multi-resolver environment • Multiple non-equivalent query paths, such as split-horizon DNS or geo-sensitive answers • Local DNS caches (e.g. partitioning, use of stale records) • Resilience and fault-tolerance (e.g. single points of failure) • Support for debugging and analysis • DNS Push (accepting responses to queries that have not yet been issued) • Ossification and evolvability

Sin embargo, el consenso, o el consenso básico, es uno de los conceptos más delicados del IETF (véase también la RFC 7282). El concepto de "consenso total" era ajeno al IETF y muchas personas se quejaron. Asimismo, la lista de temas dentro del alcance se infló en la nueva versión del acta constitutiva, y nadie expresó consentimiento sobre la lista extendida durante la sesión. Aunque hubo un consenso básico notable sobre que la lista extendida era demasiado larga, faltó moderación durante la sesión, lo que impidió cualquier tipo de progreso. Inmediatamente después de la BoF, el expresidente del IETF, Jari Arkko, aclaró el tema ofreciendo la siguiente propuesta de alcance reducido:

> **escribir una especificación que permita el descubrimiento y el uso de servidores DNS, con algo como el adaptive DNS como punto de partida*
>
> *—incluyendo el análisis de seguridad general, el análisis de los impactos en la privacidad, y el análisis sobre la resistencia a la vigilancia generalizada con respecto a esta propuesta*
>
> **usar el proceso estándar de WG del IETF*

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

Tras el fracaso de la BoF, el comienzo de un nuevo WG potencial podría darse en la reunión IETF 107. Durante la sesión, la presidenta del IETF, Alissa Cooper, remarcó que la BoF no había logrado avanzar luego de una situación en la que dos bandos se encontraban enfrentados.

El bando pro DoH/Web argumentó, por ejemplo, que no había necesidad de crear un nuevo WG, ya que estaba el WG de DNS (David Schinazi, Google, previamente de Apple). Patrick McManus (Fastly, previamente de Mozilla) dijo que el acta constitutiva carecía de especificidad. Martin Thomson (Mozilla) alertó contra un acta constitutiva de WG "tipo pulpo". En el "otro" bando, Chris Box (BT) dijo que la lista reducida podría ser demasiado corta, pero que la lista extendida era demasiado larga. Algunos, como Ralf Weber (Akamai), solicitaron un debate más estructurado en un posible WG. Dado que la BoF fue un fracaso, las partes interesadas tendrán un intento más.

¿Una guía del viajero para QUIC?

Al igual que el DoH y posiblemente el ADNS (ODNS) cambiarán el DNS, QUIC cambiará el transporte y tomará un poco del transporte tradicional del TCP. QUIC (Conexiones UDP rápidas en Internet) es un nuevo protocolo de transporte de Internet, cifrado por defecto, que intenta hacer más rápido y más seguro el transporte, y apunta a reemplazar el TCP y TLS en la web, según opinan algunos.

Actualmente, las cifras que se informaron sobre el uso de QUIC están entre el 2,6 y el 9 por ciento. En diciembre, dos documentos fundamentales del Grupo de Trabajo de QUIC procederán a la última llamada del Grupo de Trabajo:

- draft-ietf-quic-tls-24 Using TLS to Secure QUIC
- draft-ietf-quic-transport-24 QUIC: A UDP-Based Multiplexed and Secure Transport

Durante una charla oportuna en la Reunión Abierta del Área de Transporte, el copresidente de QUIC, Mark Nottingham, dijo que el grupo habilitaría una fase extendida para comentarios sobre el nuevo protocolo de transporte.

Aunque ha durado más de lo que sus defensores esperaban en un principio, el WG de QUIC ha sido, quizás, uno de los WG más intensos, con tres reuniones de WG normales durante las IETF —cada una con dos sesiones— así como también tres reuniones anuales paralelas entre las reuniones del IETF. Gracias a que las pruebas de interoperabilidad están mejorando y los *drafts* se están estabilizando, el plan actual es llevar estas propuestas al IESG a mediados de 2020, según Nottingham. Según dijo, otros documentos seguirán los pasos más o menos rápidamente de los documentos fundamentales, incluidos los siguientes:

- draft-ietf-quic-recovery-24 QUIC Loss Detection and Congestion Control
- draft-ietf-quic-qpack-11 QPACK: Header Compression for HTTP/3

y documentos sobre problemas operativos como:

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

- draft-ietf-quic-invariants-07 Version-Independent Properties of QUIC.

El WG ya está trabajando en la versión 2 de QUIC, pero Nottingham indicó que la misión del grupo, por ahora, era lanzar el protocolo base.

Como el DoH, QUIC parece subrayar que el rediseño de la red está siendo impulsado por lo que podrían ser las denominadas "compañías web". La reacción de muchas de estas empresas al desarrollo de QUIC ilustra este cambio. Nottingham presentó largas listas de extensiones y aplicaciones, algunas ya adoptadas y otras esperando llegar al WG. Según comentó, QUIC será el nuevo tema candente.

Las extensiones que considera el WG son las siguientes:

- Balanceadores de carga QUIC (duke-quic-load-balancers)
- Negociación de versión QUIC (schinazi-quic-version-negotiation)
- Datagramas QUIC (pauly-quic-datagram)
- Bits de pérdida (ferrieuxhamchaoui-tsvwg-lossbits) (documento futuro)

Nottingham también informó sobre la creciente cantidad de aplicaciones que ya han expresado interés en usar QUIC (como WebTransport, vvv-webtransport-quic, proxy/*tunnelling*, por ej., draft-schinazi-masque), así como también DNS y Netconf. El trabajo correspondiente se completará en otros WG, según Nottingham. Ya se está trabajando en "pluginised QUIC" y en QUIC para Satcom.

Con la gran cantidad de propuestas relacionadas con QUIC, se consideraron dos ideas durante la reunión. Una era habilitar un Grupo de QUIC Dispatch especial, que analizaría todos los *drafts* relacionados con QUIC y los enviaría a los WG responsables.

La otra propuesta para la preparación del despliegue de QUIC fue presentada por el presidente de la IAB, Ted Hardie, quien dijo que podría ser hora de preparar una "Guía del viajero para QUIC" para permitir que quienes lo implementen lo hagan bien desde el principio: algo que, para protocolos más antiguos, se hizo luego de la estandarización. Hardie se refirió al SIP para usarlo como modelo en la Guía del viajero.

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

Grupos de trabajo

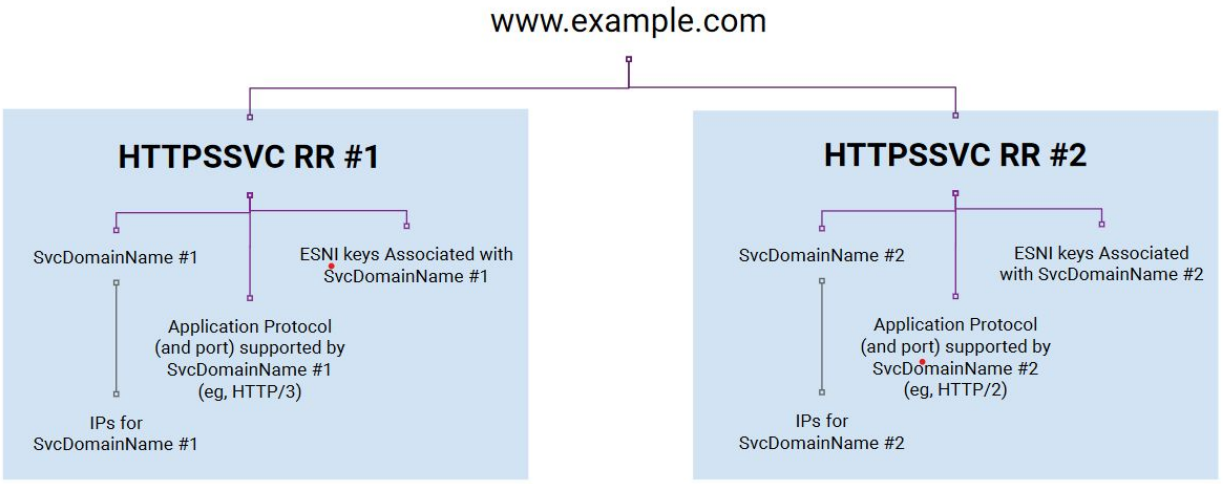
DNS: otra edición de .internal y una solución final para aname, bname y cname

Dos *drafts* en particular llamaron la atención de los expertos en DNS durante las dos sesiones del WG de DNS.

Uno tiene que ver con el intento de resolver el problema de "ANAME, DNAME, CNAME" de una sola vez. Ben Schwartz (Google) presentó un *draft* que tiene como objetivo explícito permitir que un cliente consulte un nombre y obtenga "todo el paquete de información" necesario para conectarse a un servicio. Según el autor, el nuevo registro brindará un paquete entero de información en lugar de solo una dirección IP. Funciona como CNAME, pero podría ubicarse en el APEX como un alias.

Tras presentar una solución de HTTPS, HTTPSSVC, los autores ahora también brindan una solución genérica: SVCB. Los nuevos registros permitirán la delegación de una autoridad operativa para un origen dentro del DNS a un nombre alternativo.

Según el *draft*, SVCB y HTTPSSVC habilitarán el suministro de extremos de servicios autoritativos, junto con parámetros asociados con cada uno de esos extremos "mientras reconocen diferentes respuestas a la solicitud de registro de diferentes entornos de *hosting* o CDN (multihogares) y habilitan la funcionalidad tipo CNAME en la zona apex (example.com) para los protocolos que participen". En definitiva, la propuesta, según lo que explicó Schwartz, dará paso a un *hosting* de CDN múltiples con cifrado ESNI.



Según el autor, su *draft* es una respuesta más completa al pedido de implementar SRV o un equivalente funcional en HTTP e intenta la delegación usando ALTSVC, ANAME y ESNIKEY. El problema con los variados enfoques anteriores siempre fue que terminaban en

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

incompatibilidades y, al mismo tiempo, solo resolvían una parte de las funciones, respectivamente.

En su mayor parte, el WG recibió con gusto el *draft* (por ejemplo, David Schinazi de Google, Tommy Pauly de Apple, Brian Dickson de GoDaddy, Ondrej Sury de ISC), pero quedaron preguntas por debatir. El mismo Schwartz pidió opiniones sobre dos preguntas: cómo equilibrar la rigurosidad de ESNI contra la confiabilidad y la mala configuración. Schwartz explicó que los requisitos actuales impiden el retroceso de ESNI a no ESNI, a menos que el servidor indique específicamente que lo permite. Otra pregunta tuvo que ver con la posible necesidad de limitar la longitud de cadena.

Schwartz pidió más recomendaciones de los operadores de servidores sobre el gráfico de comportamiento de servidores, tanto autoritativos como recursivos.

El comportamiento de servidores actual se describe en el *draft* de la siguiente forma:

1. *Al procesar una respuesta SVCB de un servidor autoritativo, se agrega a la Sección adicional (a menos que sea la Respuesta).*

2. *Si todos los registros están en ServiceForm, se resuelven los registros A y AAAA para cada SvcDomainName (o para el nombre del propietario si el SvcDomainName es "."), y se incluyen todos los resultados en la Sección adicional.*

3. *De lo contrario, se selecciona un registro AliasForm al azar, y se resuelven los registros A,AAAA, y SVCB para el SvcDomainName. Si el registro SVCB no existe, se agregan los registros A y AAAA a la Sección adicional. De lo contrario, se vuelve al paso 1, sujeto a la heurística de detección de loops.*

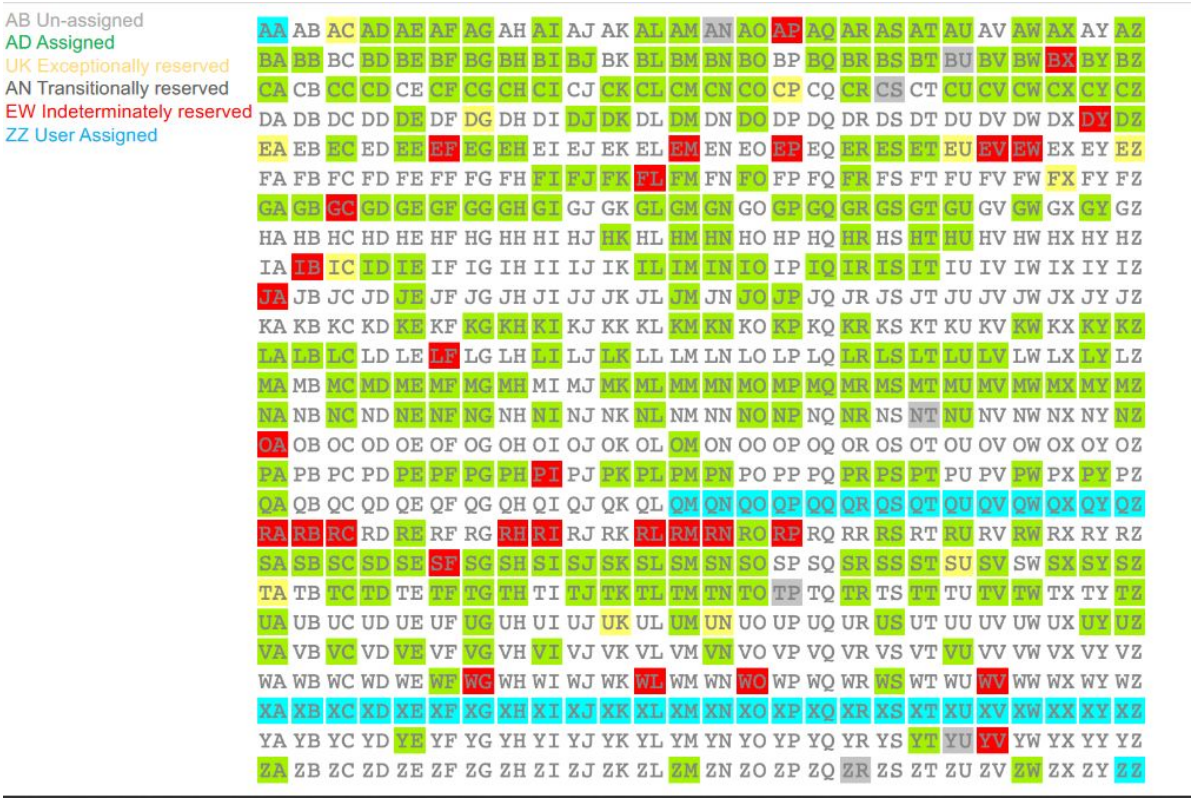
> *Todos los servidores DNS DEBERÍAN tratar a la porción SvcParam del RR de SVCB como opaca y NO DEBERÍAN intentar alterar su comportamiento en base a sus contenidos.*
>
> *Al responder a una consulta que incluye el bit OK de DNSSEC ([RFC3225]), los servidores DNS recursivos y autoritativos capacitados para DNSSEC DEBEN acompañar cada RRSet en la Sección adicional con los mismos registros relacionados con DNSSEC que enviaría al brindar ese RRSet como Respuesta.*

El WG concluyó que el *draft* tiene que estabilizarse antes de poder solicitar los nuevos tipos de registro en la IANA.

Otra propuesta muy debatida es darle otra oportunidad a una zona “interna”, que no logró conseguir apoyo cuando el IETF intentó obtener .internal o .home. Es interesante que fueron dos autores de ICANN, Roy Arends y Ed Lewis, quienes presentaron ante el IETF la nueva propuesta para una zona de direcciones interna no delegada por ICANN. Para evitar la necesidad de delegación, el IETF podría elegir un código alpha-2 no asignado de la lista ISO 3166-1, que enumera los códigos de país. Según Arends, de todos los posibles códigos alpha-2,

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

había algunos que no estaban asignados ni se esperaba que se asignaran en el futuro. De la lista (véase el gráfico a continuación), Arends y Lewis proponen seleccionar .zz.



Arends afirmó que la forma corta y la falta de semántica eran una ventaja de la etiqueta. No todos estuvieron de acuerdo con esto. Warren Kumari, autor del *draft* .internal, dijo que la falta de significado semántico confunde a los usuarios. Petr Spacek (CZ.NIC) señaló que con el tiempo seguirían ocurriendo colisiones, con empresas que se fusionan, etc. Sin embargo, dio la sensación de que la mayoría de los participantes en el WG de DNS apoyaron la idea. Todavía hay que debatir sobre el *draft* antes de tomar la decisión de adoptarlo como un documento del WG.

Otros *drafts* en los que el DNSOP está trabajando actualmente son los siguientes:

- Message Digest for DNS Zones, draft-ietf-dnsop-dns-zone-digest, Duane Wessels
- Extended DNS Errors, draft-ietf-dnsop-extended-error, Wes Hardaker
- DNS Transport over TCP - Operational Requirements, draft-ietf-dnsop-dns-tcp-requirements, Duane Wessels
- Interoperable Domain Name System (DNS) Server Cookies, draft-ietf-dnsop-server-cookies, Willem Toorop
- Related Domains By DNS, draft-brotman-rdbd, Stephen Farrell
- Operational recommendations for management of DNSSEC Validator, draft-mglt-dnsop-dnssec-validator-requirements, Daniel Migault

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

- Avoid IP fragmentation in DNS, draft-fujiwara-dnsop-avoid-fragmentation, Kazunori Fujiwara

RegEXT: aprobación automática de documentos de registro-registrador

El Grupo de Trabajo de RegEXT revivió una vez más discusiones conocidas sobre su trabajo. Una preocupación constante es que las prácticas de negocios de algunas empresas/organizaciones reciben el sello de "estándar del IETF". Durante la reunión en Singapur, el *draft* sobre registraciones en paquete, promovido durante muchos años por autores de CNNIC, recibió otro rechazo, ya que el IESG había claramente recomendado que fuera solo un documento informativo. Contra los argumentos de Ning Kong, asesor de CNNIC, sobre que los autores no querían conformarse con un mero estatus informativo, el copresidente de RegEXT, Jim Galvin, dijo que el documento no podría avanzar más si los autores no aceptaban.

Otro problema surgió cuando los presidentes del WG de RegEXT dijeron que, debido a que el documento *Registry Data Escrow Specification* había recibido solo dos respuestas, no había suficientes comentarios como para enviarlo al IESG. Hace ya algún tiempo que el WG ha estado teniendo problemas para atraer suficiente interés de las personas para que revisen los documentos. La razón es que aquellos que siguen los esfuerzos de estandarización específicos conforman un grupo muy pequeño de operadores de registro, al igual que una pequeña cantidad de registradores que pueden costear seguir el trabajo.

Adicionalmente, como mencionó Galvin al hablar de la especificación de depósitos y del documento *Domain Name Registration Data Objects Mapping*, las prácticas respectivas son obligaciones para las partes contratadas de ICANN. Por lo tanto, al estandarizar las prácticas, esto no puede hacer que el enfoque actual sea incompatible. Así, se demuestra claramente que no será bienvenida una desviación respecto de las cláusulas contractuales.

En consecuencia, hubo bastante resistencia contra una propuesta de Galvin de llevar más de una docena de prácticas diferentes usadas en la generación de informes de registro-registrador de ICANN al WG para la estandarización.

Alex Mayrhofer advirtió que estas eran meras prácticas que regían las relaciones negocio a negocio. Faltó interés público por Internet en su totalidad. Por lo tanto, consideró que este esfuerzo sería definitivamente una acción de aprobación automática y un abuso del IETF. Richard Wilhelm (Verisign) también advirtió que la comunidad de TechOps (operaciones técnicas) en ICANN no había llegado a un acuerdo sobre algunas de las prácticas. Traerlas al IETF sin realmente dar participación a la comunidad relevante en el debate significaría hacer caso omiso a los procesos de TechOps.

Finalmente, Mario Loffredo (Registro .it) presentó el progreso de tres *drafts* relacionados con el RDAP e hizo frente a preguntas sobre una adecuada sección de consideraciones de privacidad, en particular en el *draft* sobre la búsqueda inversa del RDAP.

Se debatieron brevemente dos propuestas para nuevos trabajos. Una es una propuesta anterior de ICANN, que busca estandarizar las operaciones de Trademark Clearinghouse.

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

La otra es una propuesta de Mayrhofer para estandarizar una función que habilite sugerencias de dominios a los registrantes, que, según se dijo, era innecesaria, dado que los grandes registradores ya tenían sus soluciones privadas.

GenART Dispatch: problemas de organización

El reciente GenArt Dispatch se estableció para lidiar con una serie de propuestas existentes que abordan la propia organización del trabajo en el IETF. Al mejor estilo "*dispatch*", el grupo analizará las propuestas y decidirá cómo deberían abordarse. Se decidió que todos los documentos presentados en Singapur se abordarían mejor en un documento *draft* esponsoreado por AD.

En Singapur, GenART debatió una propuesta directa de Joel Halpern, que rechaza fervientemente la creciente práctica de que el IESG apruebe documentos en el flujo de trabajo del IETF sin que se haya llegado a un consenso sobre estos. Esta práctica era un permiso para abusos, según afirmó un participante. Halpern argumentó que la RFC original no había previsto los diferentes flujos que se habían establecido (IAB, IRTF, además del IETF). El documento "propone que el IETF nunca publique ninguna RFC del flujo del IETF sin un consenso básico del IETF". El WG parece estar de acuerdo con esto, y se le pidió a la presidenta del IETF, Alissa Cooper, que adopte esta tarea.

Otra propuesta relacionada con un documento RFC fue la petición de Martin Thompson (Mozilla) de decirle adiós a la expiración de los documentos *drafts*.

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

Un debate más grande para el grupo será el asunto de participación igualitaria de los participantes remotos en el comienzo de retiro de un Director de Área. En la revisión del documento, los obstáculos para comenzar dicho retiro también se reducirán, según el *draft* actual de Subramaniam Moonsamey y John Klensin.

Límites borrosos: la relación entre el IETF y su organismo homólogo de investigación, el IRTF

Colin Perkins, el nuevo director de Internet Research Task Force (IRTF), el organismo homólogo de investigación del IETF, incluyó un debate profundo sobre la relación de los dos organismos con respecto a la agenda en Singapur. Hace cinco años, la RFC 7418 intentó explicar el rol del IRTF a los participantes del IETF que llevaban trabajo allí. Esta vez, el foco estuvo puesto sobre cómo los límites entre las dos organizaciones habían sido desdibujados por el IRTF, que se inclina cada vez más hacia los procesos del IETF.

No se exige que las investigaciones en curso en el Grupo de Investigación se documenten en RFC, y tampoco es necesario que el IRTF siga el concepto de consenso básico del IETF para adoptar documentos. En cambio, los artículos de investigación se publican como están (algunos buenos artículos de investigación cada año reciben el premio a la investigación aplicada en redes: véase a continuación), y algunas personas, como Stephen Farrell (Trinity College de Dublín y miembro de la IAB) dijeron que la falta de consenso era un signo saludable en el ámbito de la investigación.

Algunos de los posibles cambios para lograr un IRTF más independiente y enfocado en la investigación fueron la coubicación de las reuniones del IRTF con otras conferencias de investigación y el establecimiento de relaciones con otras organizaciones (incluyendo a la UIT, según recomendó un participante como ejemplo).

El expresidente del IRTF, Aaron Falk, describió varios tipos de relaciones entre los dos organismos homólogos “en estado salvaje”:

1. A veces el trabajo llegaba de un WG del IRTF a un WG especial, en forma de “una sola oportunidad”, como el WG de Anima del IETF, que derivó del Grupo de Investigación de Administración de la Red (NMRG). Otro buen ejemplo es el trabajo sobre IoT, ya que el RG de IoT ha contribuido con varios grupos de trabajo.

2. Otro tipo de relación ha surgido en el RG Crypto Forum (CFRG), que intervino como organismo experto para seleccionar conjuntos de cifrado seguros para el protocolo del IETF luego de que quedó claro que el NIST había quedado comprometido por la NSA. Ahora, el CFRG es el organismo permanente para seguir aconsejando al IETF sobre conjuntos de cifrado. Otro ejemplo del estilo es el Grupo de Investigación de Control de Congestión en Internet (ICCRG), que se convirtió en el organismo experto en las propuestas de control de congestión para el WG del Área de Transporte.

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

3. La tercera variante, mencionada por Falk, son los grupos de investigación que hacen investigaciones básicas en nuevas áreas de tecnología, como el recientemente establecido Grupo de Investigación sobre Internet Cuántica.

Según Falk, una pregunta para las discusiones actuales es si existe la necesidad de documentar los criterios y condiciones para una transferencia exitosa (y si más transferencia es un objetivo explícito). Es demasiado limitado contar solamente las RFC de contribuidores del IRTF (para algunos científicos a veces esto no es gratificante ya que las RFC no se aceptan como publicaciones comunes en algunas instituciones de investigación) o las RFC derivadas al IETF del trabajo del IRTF. “Hay otras métricas para el éxito además de la relación con el IETF”, dijo Melinda Shore, Arquitecta de Seguridad Principal en Fastly y presidenta de grupos del IETF y el IRTF.

También se debatieron los obstáculos e incentivos para que los investigadores contribuyan al IRTF (y al IETF) en relación con una presentación de Marie-José Montpetit.

Buen trabajo en el Grupo de Investigación de Evaluaciones y Mejoras de Privacidad (PEARG)

En Singapur, el relativamente nuevo PEARG presentó un buen ejemplo de cómo el trabajo de investigación del IRTF puede apoyar el trabajo de desarrollo de los participantes del IETF. Tanto una propuesta sobre la documentación de las cambiantes prácticas de *fingerprinting* como un marco de privacidad para el registro en redes pueden conformar trabajo real de desarrollo (y también operativo) de protocolos por parte de los ingenieros del IETF. Otro documento en consideración está basado en observaciones sobre los riesgos de la desanonimización que se originan de avalanchas de interferencias habilitadas por conjuntos de datos de capacitación de *machine learning*. Vea más aquí y aquí.

La próxima reunión del IETF tendrá lugar en Vancouver del 21 al 27 de marzo de 2020

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