Informe de CENTR

IETF 105

Montréal, 20 - 26 de julio 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

Panel de expertos: Las consideraciones de privacidad son imprescindibles para la estandarización

En una nueva versión de la plenaria técnica, la comunidad del IETF escuchó a dos reconocidos expertos en privacidad de EE. UU. Arvind Narayanan, profesor adjunto en la Universidad de Princeton, y Steve Bellovin, exdesarrollador del IETF durante muchos años, expresidente de la IAB y profesor en la Universidad de Columbia, instaron a la comunidad del IETF a tener en cuenta la privacidad al desarrollar estándares.

Tanto Narayanan como Bellovin expresaron que las revisiones de privacidad que ya se realizaron y las secciones sobre consideraciones de privacidad en algunas RFC estaban bien, pero Narayanan también subrayó que se podrían complementar con auditorías de implementación una vez que se apliquen los estándares. Narayanan, que también dirige el Proyecto de Rendición de Cuentas y Transparencia Web (WebTAP) de Princeton, puso énfasis en el potencial de cooperación entre los desarrolladores y los académicos en materia de privacidad. Narayanan indicó que a los académicos se los podría atraer con los precios.

El WebTAP de Princeton es un ejemplo de trabajo de auditoría. Es una plataforma de software que está curada por un grupo de investigadores y se utiliza para llevar a cabo exámenes frecuentes en millones de sitios en busca de violaciones a la privacidad, por ejemplo, la técnica de *fingerprinting* o la filtración de datos. Contrariamente a estudios anteriores que indicaban que el 90% de los usuarios era identificable mediante su navegador a través del *fingerprinting*, estudios más recientes descubrieron que esa cifra es menor, según Narayanan. “El tren no se nos pasó”, dijo, refiriéndose al *fingerprinting*. Además, dijo que los desarrolladores no estaban solos en la lucha por la privacidad, señalando la decisión de la Comisión Federal de Comercio de EE. UU. de multar a Google por burlar deliberadamente el bloqueo de Safari de las cookies de terceros en 2012.

En los últimos años, Steven Bellovin ha trabajado en la esfera política, incluso como asesor durante la administración de Obama. Instó a que los técnicos tomen en consideración el entorno político, ya que es necesario compartir el conocimiento técnico con legisladores y reguladores. Con respecto a lo que podría hacer el IETF, Bellovin también agregó que los desarrolladores deberían evitar permitir demasiada flexibilidad en la implementación de sus estándares. “Ya no se debería dejar en manos de la implementación, ya que eso es lo que después habilita el *fingerprinting*”, advirtió.

Su principal argumento en la charla sobre privacidad fue que el actual paradigma de privacidad está roto. “Ya no existe el consentimiento informado”, aseguró. El concepto, que se origina a partir de investigaciones jurídicas en la década de los 60, no ha estado a la altura de los nuevos desarrollos. Las declaraciones de privacidad a las que suscribían los usuarios eran demasiado largas y complejas. Los modelos de negocios de los corredores de datos, que ni siquiera tienen una relación contractual con los usuarios, se tomaron como ejemplo. Según Bellovin, no está claro qué podría reemplazar al consentimiento informado. Tampoco es práctica una declaración de uso, que permitiría a los usuarios declarar qué se puede hacer con sus datos. La provisión de una interfaz fácil de usar para hacer tal declaración es difícil y la ejecución, un problema.

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

Bellovin indicó que lo que se necesita, antes que nada, es un nuevo paradigma de privacidad. “Esta es una tarea de investigación”, dijo.

Bellovin hizo un breve comentario sobre el controvertido tema del DNS sobre HTTPS (DoH), subrayando su escepticismo con respecto a la agregación de tráfico que se vería favorecida con la implementación del DoH.

Posiciones consolidadas: el actual debate sobre DoH

En Montreal, tanto Mozilla como Google presentaron sus planes para DoH ante la comunidad del IETF durante la BoF de Applications Doing DNS (ADD) —y fueron bastante diferentes.

Mozilla: higiene del cifrado, el fin del DNS como punto de control

Martin Thomson (Mozilla), que también está en la IAB, anunció que la compañía se estaba preparando para implementar la tecnología con una opción de exclusión para lugares/usuarios que tengan “controles” vigentes. En resumen, si los usuarios/redes no quieren estar bajo el DoH, deben señalárselo al navegador. Según los planes actuales, las señales no serán autenticadas, lo que las expone a abusos mediante ataques de versión anterior. “Es una solución temporal”, admitió Thomson.

Sin embargo, a pesar de la considerable crítica por parte de los proveedores de red, Mozilla quiere mantener su rumbo. Si el espacio de nombres del DNS no estuviera fragmentado, la compañía ya habría lanzado el DoH, según Thomson. Sin embargo, un comienzo tardío permitió que progresara el asunto del descubrimiento de servicios.

Durante la muy concurrida sesión BoF, Thomson explicó que la razón principal de esta decisión se debió a los intentos de usar el DNS como punto de control. Indicó que los problemas como la filtración de contenidos, la detección y el bloqueo de *malware*, los portales cautivos, los servicios de acceso específicos a empresas o redes, las políticas de enrutamiento y las regulaciones son las razones por las que las aplicaciones ni siquiera querían usar el DNS en un primer momento. Muchas de las “técnicas de control” no eran funcionales, y el filtrado en base al DNS resultó en demasiado o insuficiente bloqueo.

Encender el cifrado socava el uso del DNS como punto de control, según Thomson, quien agregó que el nombrado alternativo ya estaba ocurriendo, por ejemplo, con la RFC 7838 “HTTP Alternative Services”:

> *“Los servicios alternativos no remplazan ni cambian el origen de ningún recurso dado; en general, no son visibles para el software ‘por encima’ del mecanismo de acceso. El servicio alternativo es, fundamentalmente, información de enrutamiento alternativo que también puede ser usada para llegar al origen de la misma manera que los registros DNS CNAME o SRV definen la información de enrutamiento en el nivel de resolución de nombres. Cada origen mapea a un conjunto de estas rutas —la ruta por defecto deriva del origen mismo y las otras rutas se incorporan en base a la información de servicio alternativo”.*

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

Thomson predijo que, a la larga, las aplicaciones (no solo los navegadores) querrían cifrar todo y elegir en quién confiar los datos. En ese caso, la única manera de ejercer el control sobre el tráfico sería trabajar directamente con los extremos. Las cuestiones de filtrado, monitoreo y "control en el extremo" se mencionaron varias veces en el debate siguiente. Mientras tanto, se publicó un *draft* que resultó de los debates sobre el TLS 1.3, que detalla las inquietudes de los operadores con respecto al cambio hacia monitorear y proteger los extremos solamente (en lugar de monitorear en las puertas de red).

El pedido de los operadores de permitir que los usuarios finales decidan por ellos mismos quién responde sus consultas en el proceso de resolución del DNS no se puede implementar. El DNS es parte de la "tubería" y nadie esperaría que los usuarios se ocupen de los caños en sus casas. Thomson también reiteró que la principal motivación de Mozilla era que la compañía piensa que el cifrado es higiene básica, y que la privacidad y la seguridad no deberían ser opcionales.

Inmediatamente después del IETF, Mozilla publicó un posteo de blog sobre sus planes para el DoH, que parecen un poco más cuidadosos que los expresados en la reunión del IETF en Montreal. El posteo también anunció más pruebas "para saber cuán seguido los usuarios de Firefox están sujetos a estas configuraciones de red (controles parentales). Para hacerlo, estamos llevando a cabo un estudio dentro de Firefox para usuarios en EE. UU. para recopilar indicadores que ayudarán a responder esta pregunta. Estos indicadores se basan en abordajes comunes hacia la implementación de filtros y resolutores DNS empresariales".

Google: pisando cuidadosamente

Kenji Baheux, gerente de desarrollo web y Chrome en Google, anunció un enfoque mucho más restringido. Una decisión unilateral sobre un cambio a una nueva resolución podría confundir a los usuarios que tenían ciertas expectativas sobre la resolución. "No les impondremos un cambio de proveedores de DNS a los usuarios", aseguró Baheux. Google también considera que los negocios deben estar "a cargo de la experiencia de los usuarios".

Con respecto al plan de despliegue, el Documento DoH de Google indica:

> *"No tenemos planes vigentes para desplegar el experimento descrito anteriormente a más del 1% de estabilidad. Si el experimento se desempeña bien, consideraremos un lanzamiento completo, que probablemente incluiría una UI de ajustes formales y un soporte mejorado para el modo seguro, especialmente en resolución de portal cautivo. El despliegue requeriría una nueva bandera Finch para controlar si la UI es visible.*
>
> *Por el momento, Google quiere atenerse al experimento con 5 a 10 proveedores de servicios DoH que hayan cumplido con una serie de criterios de privacidad. Si un usuario ya está usando un servidor de esa lista, 'actualizaremos al DoH con ese proveedor. Luego, se podría añadir una interfaz de usuario para elegir proveedores'".*

El "plan de prueba" publicado dice:

> *"Para el experimento del modo automático, debemos verificar que la configuración del sistema DNS esté debidamente descubierta en un dispositivo Windows real, tanto con una VPN como sin ella. También debemos confirmar de manera manual que la configuración Android DoT se lea y actualice correctamente. Antes de que lancemos oficialmente el modo seguro, debemos verificar que la resolución de portal cautivo tenga*

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

éxito en todas las plataformas para un rango de implementaciones activas de portal cautivo".

A diferencia de Mozilla, Google parece estar tomándose su tiempo para el desarrollo del DoH. No está claro si esto se debe a pedidos de operadores de red o de políticos, pero durante el debate de micrófono abierto, Baheux informó que, en comunicación con los ISP, Google entendió que seguir adelante con el DoH era simplemente insostenible. "Si la decisión está entre un mundo donde podemos llegar a un 99% de seguridad contra las amenazas cibernéticas, brindando, al mismo tiempo, a las fuerzas de aplicación de la ley 80% de lo que buscan y un mundo en el que aumentamos la ciberseguridad a un 99,5% pero no le damos acceso a las fuerzas de aplicación de la ley, la elección para la sociedad es clara".

A pesar de este enfoque cuidadoso, David Schinazi, exingeniero de Apple que ahora trabaja en Google, presentó un *draft* sobre un elemento adicional para un futuro entorno DoH. Por razones de rendimiento, recomendó que los servidores web indiquen ellos mismos a los clientes qué servidor DoH resolvería mejor sus direcciones. Por lo tanto, un origen HTTPS indicaría su preferencia con respecto al servidor DoH al que consultará el cliente con un "campo de encabezado DoH-Preference":

*DoH-Preference = doh-uri *(OWS ";" OWS parameter)*

doh-uri = quoted-string

parameter = token "=" (token / quoted-string)

El *draft* —hasta ahora— poco pulido de Schinazi, Nick Sullivan y Jesse Kipp (ambos de Cloudflare) está disponible aquí. Durante la sesión BoF de ADD, Schinazi explicó que el concepto podría usarse para mitigar los tiempos de respuesta cuando las solicitudes DoH terminan en servidores que no son óptimos para resolver nombres, por ejemplo, en una CDN en lugar de otra. Los navegadores trabajarían con una lista de servidores DoH aprobados, usarían proveedores DoH preferidos cuando se haya expresado una preferencia y cuando un servidor propuesto esté en la lista, y los proveedores de contenido podrían, ellos mismos, brindar un servidor DoH aprobado.

Uno podría preguntarse qué pasará si el desarrollo paralelo de servidores de origen implicara que las redes locales anuncien sus servidores DoH preferidos, lo que resultaría en negociaciones complicadas sobre dónde tiene que resolver finalmente la resolución DNS.

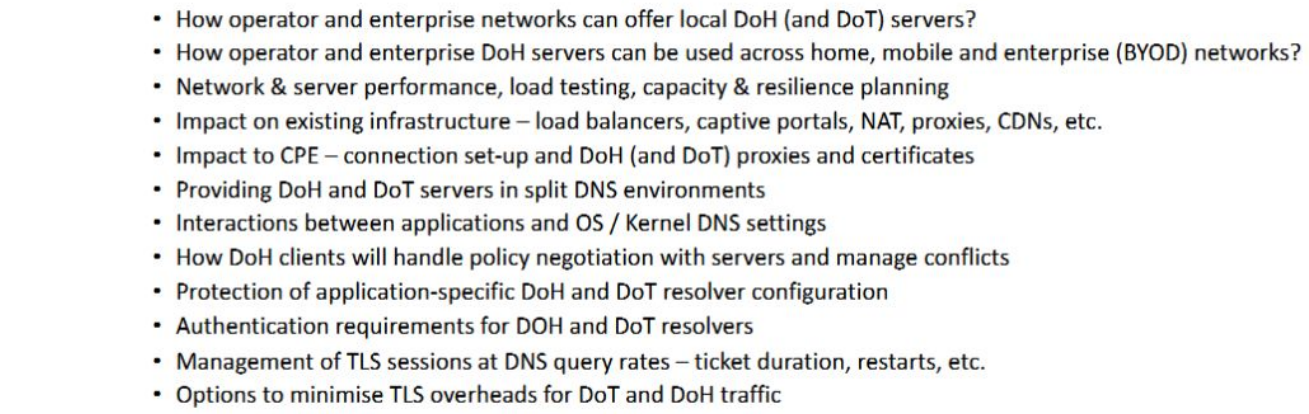
Preocupaciones de los operadores

Esta vez, a los operadores de red/ISP los representó British Telecom. Chris Box, debutante en el IETF, expuso una lista de problemas y preocupaciones que ya eran conocidas y han sido comunicadas, en especial el impacto en sus NAT, proxies, portales cautivos, balanceadores de carga y los efectos para las CDN.

Cabe mencionar que si bien el bando de HTTP-DoH (como Schinazi de Google) está intentando disipar algunas barreras acordadas como el desempeño de CDN y el descubrimiento de servicios para evitar la resolución monolítica, los operadores de red/telcos/ISP señalan que están interesados en implementar el DoH ellos mismos de manera local. Cox remarcó que no se oponía al DoH, pero quería que el IETF establezca un Grupo de Trabajo para desarrollar las prácticas recomendadas para que los operadores ejecuten los servidores DoH. No solo preguntó

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

cuál sería la mejor manera para que los operadores ejecutaran los servidores DoH de manera local, sino también si los operadores deberían poner DoH en enrutadores domésticos.



Jim Reid, también hablando desde el bando de los operadores, añadió más barreras al DoH, haciendo preguntas sobre los posibles conflictos que resulten de la fusión de los dos protocolos (HTTP y DNS). Según Reid, del lado de HTTP, el HTTP Push es un problema. Del lado del DNS, enumeró estándares como el cacheo negativo de las DNSSEC, el manejo de las solicitudes firmadas en TSIG, las actualizaciones dinámicas y otras adiciones del DNS, preguntando si los servidores DoH tendrían que implementarlos.

También remarcó la pregunta real del DNS tradicional: ¿cómo tratarán la raíz de la IANA los servidores DoH?, ¿será posible obtener diferentes respuestas según dónde se realice la resolución o las respuestas DoH diferirán del "DNS convencional" (ahora también llamado Do53)?

Pedirles a los proveedores del DoH que sean "buenos ciudadanos del DNS" mediante la implementación de las DNSSEC y otros estándares que no son obligatorios (y no están implementados) por parte de los proveedores del DNS tradicional era un pedido hipócrita, según dijo Stéphane Bortzmeyer (Afnic) a quien escribe.

Por otro lado, al presentar a la privacidad como una motivación principal, Thomson dijo que tuvieron que enfrentarse a cuestionamientos sobre su "coartada" de privacidad, ya que el DoH solo aseguraba la privacidad en el camino. Con respecto a la implementación del "Resolutor de Confianza", se tendrían que revisar las políticas de privacidad y las posibles filtraciones de los encabezados HTTP.

¿Fin del juego para el DNS? Próximos pasos

Durante la charla de Thomson, quedó claro que había una confrontación a la idea de que el DNS es una parte central de la infraestructura. Thomson argumentó que la comunidad de desarrolladores debería considerar si las funciones provistas por el DNS podrían desempeñarse

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

de otras maneras. Ya existen opciones de nombrado alternativo, según informó, haciendo un guiño a, por ejemplo, el nombrado HTTP en la RFC de Mark Nottingham.

Wes Hardaker dijo que una pregunta pendiente era: "¿Debería el IETF estandarizar el concepto de resolución de nombres hecha por aplicación, tomando una decisión o dejándolo todo en un desenlace?" Leslie Daigle cuestionó la BoF, pidiendo más consideración sobre cómo podría evolucionar el DNS y un análisis más claro de las consecuencias arquitectónicas, también mediante la definición de qué es una aplicación, cuáles son los servicios y qué es un sistema de nombres. Lorenzo Colliti (Google) también lo clasificó como un problema arquitectónico. "El problema surge cuando los clientes usan resolutores que son diferentes de los que configura la red". No era un problema del DoH; además, no había problemas técnicos con el DoH. Para algunos defensores de la serie del DoH, el actual debate con los operadores es un recordatorio de las discusiones sobre puertas traseras para los operadores y las empresas de redes en el TLS 1.3. En ambos casos, la pérdida de "puntos de control" terminó en largas discusiones.

La concentración de los flujos de tráfico del DNS —según la implementación— fue una preocupación importante planteada por varios oradores durante la BoF de ADD, incluido el expresidente del IETF, Jari Arkko, y Roland Rijswik (NLnet Labs). En un *draft* presentado para el debate emergente sobre un nuevo modelo de amenaza para el diseño de protocolos de Internet (ver más abajo), Arkko escribió que el DNS está mostrando algunos signos de vejez pero que cambiaba muy lentamente, motivando el cambio hacia el DoH. Sin embargo, Arkko advirtió que "si bien la seguridad de los intercambios reales de protocolos mejora con la incorporación de esta nueva tecnología, esto implica, al mismo tiempo, un cambio de uso desde un conjunto de resolutores DNS distribuidos en todo el mundo hacia resolutores mundiales más centralizados", lo que crea blancos bien recibidos por el monitoreo generalizado.

Los presidentes de la BoF de ADD y el IESG tendrán que tomar una decisión tras los controvertidos debates, que fueron más "civilizados" en comparación con el intercambio de opiniones en la reunión paralela del IETF104. Tendrán que tener en cuenta las siguientes preguntas prácticas: ¿debería constituirse un Grupo de Trabajo además de los de DoH, DNSOP y DPRIVE? ¿Cuál sería su ámbito?

Durante la sesión, los operadores pidieron que el IETF establezca un Grupo de Trabajo de "Preocupaciones operativas" que, según Barbara Stark (AT&T), debería tener un copresidente de la comunidad de los operadores. Stark advirtió que el DoH había pasado a ser una de las preocupaciones principales con respecto a los cambios necesarios de redes y el aumento de los costos de resolución de problemas.

Muchos del bando del HTTP cuestionaron la necesidad de un grupo de trabajo adicional, remarcando que ya había varios grupos de trabajo abordando el DNS. De hecho, Stephen Farrell dijo que había sido un error separar el DoH y el DPRIVE —ambos están preparando sus propias versiones de la privacidad del DNS.

Ben Schwartz (Google) señaló que ya había un Grupo de Trabajo de operadores de DNS, el Grupo de Trabajo de DNSOP, aunque este grupo estaba priorizando la producción de nuevas RFC en lugar de centrarse en los problemas operativos. Ted Hardie, presidente de la IAB, dijo que se podrían desarrollar varias BCP respecto del proceso de elección de un resolutor y transporte.

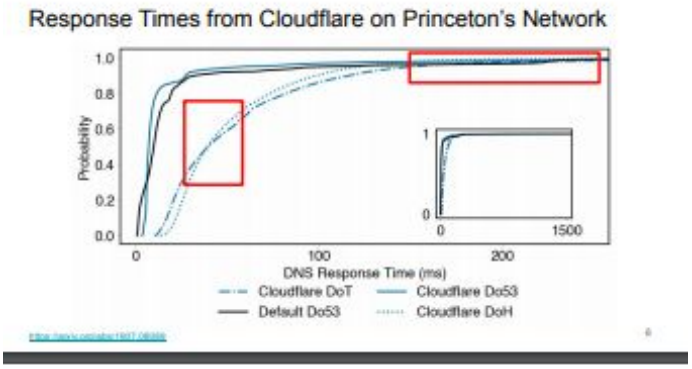
Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

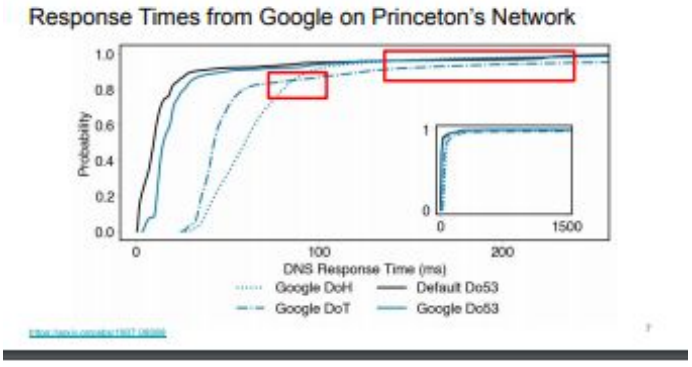
Tras la reunión del IETF, la lista de correo electrónico de ADD se ha descontrolado, y contiene una gran cantidad de posteos.

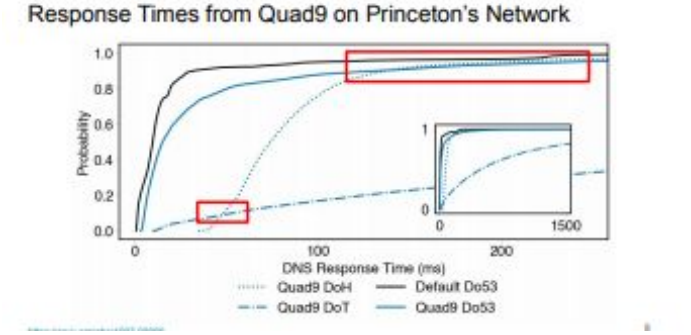
Hasta ahora, no queda claro si el IETF formará un Grupo de Trabajo de ADD o si reconsiderará cómo (y en cuántos grupos) se debería llevar a cabo el trabajo sobre el DNS en el IETF.

¿Cuán veloz es el DoH?

Con la atención cada vez más puesta en el DoH, se están llevando a cabo los primeros estudios de su desempeño. Durante el taller de Investigación Aplicada de la Red, que tuvo lugar a la par del IETF, se presentó una comparación sobre la latencia del DoH y la del DoT y Do53 (como se está llamando al DNS normal). Según la capacidad de la red del proveedor de DoH, el DNS cifrado puede ser más rápido que el DNS normal, curiosamente con el DoT teniendo un mejor desempeño que el DoH en varias configuraciones (ver el gráfico).

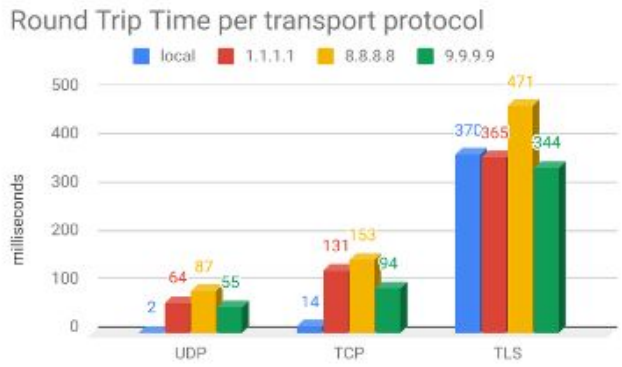






Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Los observadores notaron que las cifras dadas debían ser tratadas con precaución, ya que los investigadores habían realizado las pruebas en el laboratorio de su Universidad en Princeton. Una verificación reciente que usó sondas de RIPE Atlas y midió los tiempos de respuesta del DNS de África en la Cumbre de África reveló que, en el UDP, los resolutores locales respondieron 27 veces más rápido que los resolutores de la nube (Cloudflare, Google, Quad9). Midiendo el DoT, descubrieron que su tiempo de respuesta era tres veces más largo que el de TCP en los proveedores DNS en la nube.



Un nuevo modelo de amenaza: ataques en dispositivos y sistemas de usuarios finales

Cuatro miembros de la IAB pidieron, aunque no en representación de la IAB, que la comunidad reconsiderara el modelo de amenaza para el que fueron desarrollados los protocolos de IETF. Durante la Reunión Abierta del Área de Seguridad en Montreal, el exdirector del Área de Seguridad, Stephen Farrell (Trinity College), y el expresidente de IETF, Jari Arkko (Ericsson), presentaron algunas de las ideas.

Según Farrell, durante muchos años, el modelo de amenaza que los desarrolladores tuvieron en mente fue que los atacantes tomaran control total de la red (camino), esperando que los dispositivos no estén comprometidos. Hace varios años, y especialmente desde las revelaciones de Snowden en 2013, los desarrolladores de IETF han mejorado la seguridad de las comunicaciones, por ejemplo, mediante el cifrado del transporte (paquetes en el camino) a través de TLS 1.3 o Quic, el casi completo nuevo protocolo de transporte basado en UDP, mediante el cifrado de consultas DNS (DoT, DoH) y el cifrado de los Nombres de Dominios del Servidor (ESNI).

Impulsados, en parte, por este cierre y para burlar el cifrado, los atacantes recurrieron a los proveedores para obtener los datos —con la ayuda del capitalismo de vigilancia— o se hicieron de los dispositivos de usuarios finales. En su *draft* sobre “Cambios en el modelo de amenaza de Internet”, Jari Arkko advierte en contra de continuar centrándose solo en la seguridad de las comunicaciones, ya que esto podría “llevar a un impacto accidental o aumentado de los problemas de seguridad en los demás lugares”.

Por ejemplo, permitir la recopilación de datos mediante el diseño de protocolos incluso por partes no sospechosas implicaría que “con el tiempo, la información innecesaria se podría usar con todas las desventajas asociadas, independientemente de qué expectativas de despliegue había

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

durante el diseño de los protocolos". Arkko menciona la agregación, consolidación y concentración del tráfico (como en las implementaciones de DoH) como algunos de los problemas que requieren atención: "Es difícil imaginar que los resolutores DNS no serían el blanco de muchos ataques futuros o de proyectos de monitoreo generalizado", escribió Arkko en el *draft*, observando que "hay poco que incluso los grandes proveedores de servicios puedan hacer para rechazar el monitoreo generalizado sancionado por autoridades".

Arkko prevé las siguientes posibles pautas:

- *Considerar principios en la protección de la información y sistemas*
- *Minimizar la información que se envía a terceros*
- *Establecer una protección de extremo a extremo mediante terceros*
- *Minimizar la delegación de funciones de control a terceros*
- *Evitar los recursos centralizados*
- *Contar con acuerdos explícitos*
- *Sospechar de partes a las que se conecte tu dispositivo*
- *Cifrar todo para todos*

Farrell, autor de un segundo documento, tiene otro conjunto de recomendaciones interesantes:

- *Desarrollar una BCP para las consideraciones de privacidad*
- *Considerar no solo los casos de uso, sino también los de abuso al momento de desarrollar*
- *Reconsiderar el permitir "extensiones" de protocolos*
- *Considerar el aislamiento (para proteger contra la enlazabilidad)*
- *Popularizar el concepto de transparencia tomado por la transparencia de certificado, implementado en el GDPR*
- *Si las aplicaciones no ven los datos, es más difícil que se comporten mal (minimizar)*
- *Política del mismo origen*
- *Generalizar el modelo de amenaza de Oauth (dos de tres partes podrían colisionar contra la tercera)*
- *Actualizar el modelo de amenaza del extremo de "no comprometido" a "en general no comprometido"*
- *Reevaluar la seguridad de transporte/comunicación*
- *La recuperación ante ataques debe ser parte del diseño de protocolos*
- *Los extremos de los protocolos podrían no ser "hosts" en el sentido clásico*

Se dio un comienzo a estos debates en el taller de la IAB sobre Expectativas de Diseño y Realidades de Despliegue, que abarcó una gran cantidad de temas interesantes, algunos relacionados con el DNS, como "Tres tipos de concentraciones en los protocolos abiertos" de Andrew Sullivan.

El pedido de Farrell y Arkko recibió críticas mezcladas en Montreal. Varios participantes subrayaron la necesidad de centrarse en la implementación de los muchos estándares de seguridad y cifrado aprobados por el IETF en los últimos años en lugar de producir otra serie de documentos. Muchos hicieron referencia al trabajo en curso, por ejemplo, el nuevo Grupo de Trabajo sobre "Procedimientos de Certificación Remota" (RATS), cuyo objetivo es proporcionar un mecanismo para "evaluar la fiabilidad del par", un tipo de verificación de confianza para los sistemas remotos.

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

Sin embargo, otros recibieron con gusto los *drafts* de Farrell y Arkko, en especial aquellos que trabajan en el grupo SMART o en colaboración con este (que todavía no formuló su carta constitutiva). La gente de SMART se ocupa, principalmente, de cómo resolver los problemas que causa el cifrado para el monitoreo (de seguridad). Arnaud Taddei, de Symantec, anunció su *draft* sobre limitaciones en el extremo con respecto al monitoreo de seguridad.

Farrell intentó dejar en claro que las consideraciones del modelo de seguridad no deben resultar en el cuestionamiento de la seguridad de las comunicaciones. En su lugar, había que desarrollar más exhaustivamente el cifrado de los protocolos de comunicación.

También cabe mencionar que prestar atención a la seguridad de los dispositivos finales es un cambio de práctica respecto de las actividades usuales del IETF. Los dispositivos finales (y los usuarios finales) no entran en el ámbito de la estandarización del IETF, según recordó Daniel Kahn Gilmore a los participantes de la reunión del Área de Seguridad. Será fascinante ver si se descubre otro mantra del IETF, como recomendó Mark Nottingham, miembro de la IAB, con un *draft* informativo sobre por qué el IETF debería mantener la mirada en los usuarios y decidir en base a sus intereses en tiempos de consideraciones incompatibles.

El IETF en modo crisis

La Sesión Plenaria Administrativa en Montreal estaba preparada para debates largos y muy tensos sobre tres temas controversiales: la conducta del IETF, las decisiones presupuestarias de la LLC, y la inesperada renuncia de la editora de la Serie RFC.

Una vez más, la presidenta del IETF, Alissa Cooper, habló sobre el código de conducta del IETF, que se pulió en los últimos años, en parte debido a intercambios irrespetuosos en las listas de correo electrónico del IETF. En varias reuniones, se mencionó el problema del lenguaje rudo y el comportamiento agresivo en los grupos de trabajo y las listas de correo electrónico. La presidenta del IETF mencionó varias iniciativas recientes dedicadas a mitigar las posibles violaciones de la “buena conducta”, que incluyen debates sobre los directores de área y los presidentes de los grupos de trabajo, asistencia por parte de capacitadores profesionales, y la incorporación de más oficiales de orden rotativos que intervengan en caso de comportamiento agresivo. Tras un reciente incidente que involucró la intervención de un oficial del orden, Cooper también dijo que podría ser necesario aclarar los procedimientos sobre la intensificación de conflictos. Algunos mencionaron la posibilidad de incorporar mecanismos para lidiar con el acoso sexual (propuesta de Kristy Paine, del National Cyber Security Center). En un acto poco usual, dos miembros de la IAB, Martin Thomson y Mark Nottingham, se disculparon por las violaciones al código de conducta que ellos hubieren cometido o por su falta de intervención ante comportamiento agresivo.

El Comité Supervisor de la Serie RFC (RSOC) también envió una disculpa apenas unas horas antes de la reunión plenaria. Estaba dirigida a Heather Flanagan y concernía su decisión de no renovar su contrato como editora de la Serie RFC (RSE).

Las RFC son las producciones más importantes del IETF y se publican en diferentes corrientes: Estándares de Internet y Estándares Propuestos, las RFC del IRTF y de la IAB, y, finalmente, las presentaciones independientes (ver el sitio del editor de las RFC). Desde que asumió el trabajo en 2012, Flanagan había comenzado a trabajar en el formato de las RFC (ver los varios pasos del proceso aquí).

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

Flanagan anunció su renuncia tras confrontarse con el anuncio del RSOC para llamar a ofertas para la función del RSE antes de la posible próxima extensión del contrato actual de Flanagan (renovable en 2021 por otros dos años). Según algunas opiniones (incluidas las del RSOC), ella decidió renunciar porque interpretó que el comienzo temprano del proceso de oferta era una consecuencia de su desempeño. En la carta de disculpas, la presidenta del RSOC, Sarah Banks, explicó que la poca cantidad de candidatos en ofertas anteriores para las funciones del IETF fue lo que motivó la decisión y que, en retrospectiva, había sido una mala jugada y, obviamente, se había comunicado incorrectamente.

Flanagan le dijo a quien escribe que su decisión estaba motivada por las "demasiadas cargas administrativas" de su trabajo.

Flanagan ha supervisado la producción de la Serie RFC desde 2012. La producción se lleva a cabo por parte del centro de producciones de RFC, un grupo de editores de AMS, que están vinculados por contratos que son independientes de los contratos de RSE. AMS también es el operador de la secretaría del IETF. Además de la división contractual, también hay una división de supervisión, ya que, además del RSOC (que es designado por la IAB), también existe un Grupo Consultivo para las RFC, que, según el sitio, es nombrado por el RSE. En su declaración en la lista de correo electrónico, Flanagan señaló varios problemas:

> *"En el último año, he visto la concreción de la BoF de rfcplusplus, contra mi recomendación. Mi comité supervisor, que es un grupo con el que debo trabajar más estrechamente, fue reemplazado casi por completo sin contribuciones de mi parte. Cuento con lo que, fundamentalmente, actúa como un equipo de diseño: el Grupo Consultivo para la Serie RFC. A ellos tampoco se les consulta, por lo general. El RSOC/la IAB está presionando fuerte con respecto al SLA faltante, sin reconocer que esas declaraciones se hicieron (con todo el apoyo y comprensión de equipos directivos anteriores) en la etapa plenaria y en reuniones en que el SLA faltaría como herramienta de prueba de formato y la transición se incrementó".*

Debido a la reforma en curso y el próximo cambio al nuevo formato de RFC, el SLA no se ha cumplido últimamente, lo que también llevó a una decisión de la LLC de añadir personal al centro de producción de AMS de las RFC.

El presidente de la IAB, Ted Hardie, había delineado aquí las opiniones de la IAB y los pasos para el proceso de oferta que ahora se necesita urgentemente. Durante el debate en la plenaria, la mayoría favoreció la sugerencia de buscar un sucesor inmediatamente, y, al mismo tiempo, revaluar el constructo y las fuentes de tensión actuales.

Una de las mayores fuentes de tensión en la reunión fue la gran cantidad de opiniones diversas de los participantes del IETF sobre el RSE. Para aquellos que hace tiempo que contribuyen en el IETF, el editor es un miembro de la comunidad y una parte en el proceso, y actúa, en cierta forma, de manera independiente. Para los participantes más nuevos del IETF, muchos de los cuales ascendieron en la IAB, el RSE se asemeja más a un empleado. Varios miembros de ese grupo hicieron comentarios como para pasar a otro tema, mientras que los participantes más antiguos vieron la renuncia de la RSE como un fracaso fundamental del equipo directivo actual del IETF. Todavía están en curso los debates sobre cómo proceder, con la presión del cambio de formato y de la demora de la producción de RFC.

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

La LLC también se vio desafiada y recibió su primer “bautismo de fuego” sobre preguntas presupuestarias. Según el presidente de la LLC, Jason Livingood, en los primeros cuatro meses, la Junta Directiva de la LLC había planificado contratar un director ejecutivo (se recibieron 134 postulaciones), había elaborado sus propias políticas procesales (que están en proceso de consulta aquí), debió revisar las normas de exportación de EE. UU. y extender los contratos con el servicio de secretaría y el actual director ejecutivo interino. También se hizo cargo de las Donaciones IETF provenientes de ISOC (aproximadamente $3 millones). Leslie Daigle (al igual que Harald Alvestrand) advirtió sobre la microgestión de la LLC al reexaminar los contratos rescindidos a fin de simplificarlos. A la pregunta decisiva para las RFC la hizo Bob Hinden, quien instó a la LLC a subir los gastos $1,6 millones en 2019 con respecto al año anterior. Cooper rechazó la noción de que no se había anunciado el aumento a la comunidad y dijo que el presupuesto había sido incrementado todos los años, aunque no en una proporción tan grande cada vez.

Estos debates parecen demostrar que el IETF se encuentra ante una serie de puntos de inflexión con respecto a cómo la comunidad se gobernará a sí misma (incluyendo las consideraciones sobre reducir las reuniones y comunicarse de manera remota por razones ecológicas). Además de las tensiones dentro de la comunidad sobre los procedimientos, también surgieron tensiones entre los contribuyentes establecidos del IETF y los nuevos grupos sobre el trabajo actual o la presentación de nuevo trabajo relacionado para obtener la impronta de RFC (ver las operaciones de medios, la BoF de MOPS, los MEDUP orientados al usuario final y la comunidad de aplicación de la ley orientada a las reuniones paralelas SMART). Los nuevos grupos no se sienten bienvenidos debido a que los contribuyentes más establecidos empujan hacia atrás: de ahí surgen los problemas de conducta. Un participante pesimista le dijo a quien escribe que, en relación con el problema del RSE, el IETF tenía mucho por hacer para asegurarse de seguir funcionando.

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

Grupos de Trabajo y reuniones BoF

Grupo de Trabajo de DNSOP: Más gotas llenando el vaso, o cómo evitar temas políticamente sensibles

El Grupo de Trabajo de DNSOP recibió un pequeño golpe durante la BoF de ADD cuando Ben Schwartz (Jigsaw/Google) señaló que algunos aspectos del DoH, como las preocupaciones operativas, en realidad, se corresponderían con las funciones del Grupo de Trabajo de "Operaciones del DNS". Hasta el momento, el Grupo se las había arreglado para evitar la mayor parte del debate sobre el DoH. Ahora, tiene que adoptar un *draft* relacionado con el DoH. Es un *draft* sobre la autopublicación de qué tipo de resolución cifrada quiere ofrecer un resolutor. Otro tema altamente político, los nombres alternativos, también tuvo su breve debate en Montreal, en el que la copresidenta de DNSOP, Suzanne Woolf, consideró pedirle al IESG que haga la revisión final sobre qué hacer con el documento sobre nombres alternativos. Una vez más, el Grupo de Trabajo del DNS llenó con más y más gotas su vaso durante dos sesiones de grupos de trabajo, con una extensa lista de documentos del grupo actualmente activos y otros tantos para asumir.

Bucle de ruteo en el nombrado alternativo

En su primera sesión en Montreal, el Grupo de Trabajo de Operaciones del DNS se metió brevemente en uno de los temas más controversiales que se había pospuesto varias veces: el de los nombres alternativos. Lo trajeron a colación varias aplicaciones que se presentaron en el IETF en base a la RFC 6761 (Dominios de uso especial). Si bien algunas aplicaciones, en particular .tor, se aceptaron (con .local de Apple como el caso de uso original), se dio un intenso debate sobre la posibilidad de que el IETF conceda derechos a más dominios especiales. Muchos participantes sintieron que esta era una invitación a que las partes burlen las políticas de aplicación de gTLD de ICANN, y temieron que el IETF se metiera en un lío con ICANN por este tema.

Un documento que intenta "acorralar" a casos de uso alternativos como .tor (o .home, que recientemente se convirtió en home.arpa) en un TLD .alt se encuentra, actualmente, es su versión número 11. Durante la sesión, el copresidente de DNSOP, Tim Wiczinski, propuso enviar el documento a los directores de área del Área de Internet o del Área General para que lo "golpeen" un poco más. Sin embargo, muchos participantes, como el coautor Andrew Sullivan (ahora CEO de ISOC), pidieron a los presidentes de los Grupos de Trabajo que tomaran una decisión en lugar de crear lo que, irónicamente, sería un "bucle de ruteo perfecto". Paul Vixie, fundador de ISC y desarrollador de BIND, recomendó que el Grupo de Trabajo documente una decisión y, que si decidía no permitir dichos usos alternativos, enumere las razones de tal decisión.

Un poco de DoH en el DNS

Llegó trabajo relacionado con el DoH al Grupo de Trabajo del DNS con un *draft* que especifica la autopublicación de información de resolutores DNS, incluido el par nombre-valor del DoH necesario para permitir que los servidores expresen lo que proveen para estandarizarlos en otros sitios. En lugar de limitar esto a la información sobre el servicio DoH existente por el resolutor

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

(local) correspondiente, los autores (Paul Hoffman y Roy Arends, de ICANN y Puneet Sood, Google) optaron por generalizar el método, permitiendo que los resolutores anuncien información adicional.

Se debatieron opciones de formato para abordar el resolutor, y quedan dos en pie: in-addr/IPv6.arpa o la URI https:/.well-known/info. La idea de usar un dominio de uso especial, lo cual algunos participantes dirían que es preferible, no se perseguiría, según los autores. El *draft* establece un tipo de registro de recurso nuevo: "RESINFO". El formato elegido es I-JSON, ya que los autores piensan que sería mejor que JSON por motivos de interoperabilidad.

Durante el debate, algunos participantes cuestionaron la necesidad de estandarizar esto. Por ejemplo, Stéphane Bortzmeyer (Afnic) preguntó por qué no debería uno confiar en los mecanismos de aprovisionamiento de dominios normales que se desarrollan actualmente en el Área de Internet. Otros advirtieron sobre tamaños de registro potencialmente gigantes que podrían evolucionar con el tiempo, dado que la autopublicación es extensible. El Grupo de Trabajo aún debe decidir si quiere asumir esta tarea.

Más trabajo sobre el DoH se llevó a cabo durante la Hackatón. Petr Špaček (CZ.NIC) escribió una implementación de proxy de DoH en fastcgi, y Witold Krecicki está preparando el BIND9 para DoT y DoH.

Más decisiones por tomar: ¿HTTPSSVC en lugar de ANAME?

El largo debate sobre ANAME o una solución alternativa para simplificar las opciones de búsquedas para conectarse a URI de HTTPS dio un giro en Montreal con la presentación de una propuesta para un nuevo tipo de registro del DNS: HTTPSSVC. Los registros HTTPSSVC permitirían que los nombres de host de origen HTTPS se sirvan a partir de múltiples servicios de red. Según Erik Vyncke (Akamai), coautor con su colega Mike Bishop y Ben Schwartz (Google), cada uno puede enriquecerse con información sobre el protocolo de transporte y material de sistema de llaves para cifrar el SNI de TLS (ESNI). HTTPSSVC brindaría una solución a la incapacidad del DNS de permitir ubicar un CNAME en el ápex de un nombre de dominio. A su vez, la información en el registro permitiría la omisión del *bootstrapping* de http para todos los dominios que ofrezcan HTTPS y les ofrecería a los clientes la oportunidad de conocer todos los servicios alternativos disponibles en el origen antes del primer contacto. Según el autor, el registro mejoraría el desempeño y la privacidad.

Por el momento, el copresidente de DNSOP, Benno Overeinder, dijo que se trabajaría en el *draft* de ANAME, pero que con el interés del grupo de navegadores (tanto Erik Rescorla de Mozilla como Eric Orth de Google expresaron un claro interés durante la reunión), parecía que el "ganador" ya era HTTPSSVC. No obstante, Orth dijo que pensaba que su implementación estaba ligada al DoH, ya que estaba preocupado por enviar consultas adicionales por cada solicitud. ANAME podría seguir siendo una opción para el DNS clásico.

Algunas preocupaciones que se volvieron a mencionar incluyeron el tamaño potencial al que podrían llegar las respuestas DNS, que se podría llegar a usar para ataques DDoS (Warren Kumari, Google). Olafur Gudmundsson recomendó evitar la subtipificación, que actualmente está prevista en el *draft*, y dijo que, en cambio, se debería usar un formato con una cadena extensible en el final.

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

Falta decidir si el *draft* estará a cargo del Grupo de Trabajo del DNS, del TLS o de uno distinto.

Cerca de la última llamada: terminología y la ejecución local de un servidor raíz

Los *drafts* que están cerca de las últimas llamadas de Grupo de Trabajo incluyen la ejecución local de un servidor raíz (que puede ayudar a mitigar los riesgos de privacidad) y el documento de Terminología del DNS elaborado por Paul Hofmann (ICANN). Para el primero, se prometió una versión final para finales del mes antes de la última llamada del Grupo de Trabajo. Para el último, varios participantes pidieron apoyar la versión "ter", ya que estaría sujeta a actualizaciones de igual manera en el futuro.

Drafts adicionales

Se está llevando a cabo más trabajo para hacer que las cookies del DNS sean interoperables, con la fusión de dos *drafts* sobre cookies del DNS. Como informó durante la reunión Willem Toorop (NLnet Labs), uno de los autores de la inminente fusión de los nuevos *drafts* sobre cookies, los problemas de interoperabilidad de diferentes software de servidores DNS también se abordaron durante la Hackatón.

Otros dos *drafts* que están listos para que los empiecen a trabajar son el *draft* para evitar la fragmentación IP del DNS, por Kazunori Fujiwara, y también las recomendaciones para el comportamiento del servidor autoritativo, desarrolladas por Giovanne Moura (SIDN) a partir de un estudio sobre el tema. Dos *drafts* adicionales que se debatieron brevemente fueron el *draft* "Dominios relacionados del DNS" de Brotman y Farrell, y el *draft* sobre registro de recursos para transferir información encubierta de un servidor DNS primario a uno secundario de ISC.

REGEXT: se necesitan más debates sobre privacidad, la doble corriente entre EPP y RDAP

El Grupo de Trabajo de REGEXT debatió si debería promover estándares del RDAP adicionales o esperar a que los registros y registradores obtengan experiencia con la implementación de protocolo sucesor de "Whois". También continúa luchando con cómo abordar la privacidad en estándares relacionados con el registro, y revaluó brevemente las preguntas para el RDAP y el trabajo continuo del EPP.

A partir del 26 de agosto, los registradores y los registros de ICANN tendrán que usar el RDAP para los datos de registro (Whois), algo que hizo que Richard Wilhelm (Verisign) cuestione la necesidad de la rápida estandarización de funciones adicionales en el proceso del IETF y del impulso para el rápido despliegue.

Durante la reunión del Grupo de Trabajo de REGEXT, se presentaron cuatro *drafts* (funciones) adicionales. Los dos primeros estaban relacionados con los depósitos ("escrow"). El depósito de datos es necesario y, para los registradores y registros de ICANN, está sujeto a obligaciones contractuales: lo usan ICANN, sus registros de TLD y los operadores de EBERO. Los dos documentos se dividen en el depósito de datos y en el formato especial para los datos de registro de nombres de dominio (Registry Data Escrow Specification y Domain Name Registration Data Objects Mapping, respectivamente). Según Francisco Arias (ICANN), ambos

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

son extensibles. La división entre depósito y formato de depósito permitiría la generalización de la parte del depósito y su uso para otros conjuntos de datos.

El documento de formato define la estructura para los datos a depositar para el caso de nombres de dominio, que incluye los siguientes objetos:

Dominio
Host
Contacto
Registrador
NNDN (usado para nombres de dominio reservados, variantes de IDN retenidas, etc.)
Parámetros del EPP
Referencia de tabla de IDN
Encabezado
Políticas

Los otros dos documentos, escritos y presentados por Manuel Loffredo (Registro .IT) tienen que ver con el ordenamiento y la paginación, y también con la controvertida búsqueda inversa. El *draft* de ordenamiento y paginación tiene como objetivo reducir las necesidades de ancho de banda y los tiempos de respuesta. La búsqueda inversa permitiría la extracción de información sobre usuarios para encontrar nombres de dominio de propiedad de un individuo o compañía, comenzando con los datos del propietario, como el nombre o la dirección de correo electrónico.

Según Arias, si bien los *drafts* sobre depósitos existen hace ya un tiempo, y James Gould de Verisign recomendó un periodo de implementación, el ordenamiento, la paginación y la búsqueda inversa son más recientes.

El problema de la privacidad se habló en ambos temas. Wilhelm dijo que, ya que los *drafts* sobre depósitos estaban trabajando con PII, veía necesario debatir con más detalle los problemas de privacidad. Para la búsqueda inversa, varias personas, incluido Stéphane Bortzmeyer (Afnic), notaron que los autores casi no habían tenido en cuenta los comentarios en la sección de consideraciones sobre privacidad. En lugar de indicar que los registros/registradores “deberían” seguir las leyes locales con respecto a la privacidad, la nueva versión tiene que indicar que “deben” hacerlo. Seguir la ley se daba por sentado. Algunas adiciones que fueron pasadas por alto incluyeron las explicaciones sobre potenciales “casos de abuso” (algo que propuso Stephen Farrell en el debate sobre el nuevo modelo de amenazas [ver los aspectos destacados]).

Loffredo argumentó que la búsqueda inversa ya era posible en Whois y se ofrecía de manera comercial. Dijo que esperaba que ese fuera el caso también para el RDAP pronto. Sin embargo, esto pondría a los proveedores correspondientes (aquellos que permitan ese uso y aquellos que vendan los resultados de la búsqueda inversa) en conflicto con el GDPR de la UE.

El presidente de REGEXT, Jim Galvin (Afilias), estuvo de acuerdo con que había una necesidad de debatir más a fondo la privacidad en el Grupo de Trabajo y las consideraciones de privacidad en los textos. El Grupo de Trabajo estaba dividido en la pregunta de si tendría sentido incorporar nuevas funciones sin esperar que se alineen las políticas de ICANN o si la estandarización de las nuevas funciones debería quedar pausada hasta que se haya obtenido la experiencia con el RDAP luego del 26 de agosto.

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

¿Qué podría salir mal con el RDAP (y otras implementaciones del estándar)?

Marc Blanchet, Viagenie, marcó los errores en la implementación del RDAP, presentando una extensa lista de fallas encontradas en el ámbito por parte de los registros/registradores gTLD de ICANN y los registros IP. En la lista, Blanchet encontró valores del RDAP inexistentes o incorrectos en la base de datos, como *objeto truncado debido a política del servidor* en lugar de *objeto truncado debido a autorización del servidor*. Otros errores incluyeron enlaces autorreferenciales que crearon un bucle de solicitudes o servidores RDAP que no aceptaban el código porciento.

Además de enumerar tales errores de implementación, Blanchet también hizo recomendaciones para que la actualización del estándar del RDAP incorpore, por ejemplo, un objeto rol para los registros y para que el intercambio de recursos de origen cruzado (CORS) pase a ser una obligación en lugar de una recomendación (de un "debería" a un "debe").

Blanchet le preguntó al Grupo de Trabajo cómo seguir si, por ejemplo, debería nombrar a los responsables de las implementaciones defectuosas, y si el documento debería anexarse a un documento de BCP para los implementadores. Hablando con quien escribe justo antes del IETF, uno de los registradores de ICANN que tenía que implementar el RDAP para el 26 de agosto dijo que esperaba unas semanas ajetreadas tras el cambio de protocolo (de Whois a RDAP). Queda más trabajo para la estandarización del RDAP por delante, no solo con respecto a las nuevas funciones planificadas, sino también para las posibles actualizaciones.

EPP – RDAP: ¿una o dos corrientes?

George Michaelson (APNIC) reiteró la pregunta que se hizo por primera vez en el IETF104 sobre si la comunidad estaba considerando dividir el trabajo del Grupo de Trabajo de REGEXT. Algunos piensan que, dada la inminente ola de *drafts* del RDAP, sería útil establecer un Grupo de Trabajo adicional, en lugar de mantener juntos el RDAP y el EPP. Ulrich Wisser (Swedish Internet Foundation) les recordó a los participantes en Montreal que había motivos para mantener juntas a las dos corrientes, en particular el hecho de que el grupo ya era pequeño y que un segundo Grupo de Trabajo reuniría a las mismas personas.

El único documento de EPP presentado durante la reunión IETF105 fue el de "Secure Authorization Information for Transfers" (presentado por James Gould, Verisign). Este *draft* "define una práctica operativa, utilizando las RFC de EPP, que aprovecha el uso de valores de autorización con aleatoriedad fuerte y de corta duración, que no son almacenados por el cliente, y que se almacenan usando un *hash* criptográfico por parte del servidor para brindar un uso de información de autorización segura para las transferencias". Varios participantes hicieron referencias a sus propias implementaciones de dichos mecanismos.

Las RFC publicadas por REGEXT desde la reunión IETF105 incluyen el de "Change poll extensions for EPP, EPP organizational mapping" (RFC8543) y "Organization Extension for EPP" (RFC8544). El IESG está considerando las siguientes: Registry Fee Extension for the Extensible Provisioning Protocol (EPP) y Extensible Provisioning Protocol (EPP) Domain Name Mapping Extension for Strict Bundling Registration (informativa). En la última llamada del Grupo de Trabajo se encuentra: Login Security Extension for EPP.

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

DPRIVE: trabajo sobre privacidad, dudas sobre el descubrimiento en DoT/DoH, transferencias de zonas privadas

El Grupo de Trabajo de DPRIVE sigue considerando asegurar el próximo paso de resolución: del resolutor DNS al servidor de nombres autoritativo. Al mismo tiempo, las ideas adicionales para asegurar las transferencias de zona terminaron en críticas sobre propuestas demasiado complicadas.

El Grupo de Trabajo de Intercambio de Privacidad del DNS (DPRIVE) cubrió terreno conocido con el documento "Recommendations for DNS Privacy Service Operators", próximo a la última llamada. Este documento enumera las consideraciones y amenazas a la privacidad en las diferentes especificaciones cifradas del DNS (DoT, DoH). Según Roland Rijswijk-Deij, los autores han tomado una decisión en contra de la división de la guía para los operadores de privacidad del DNS y la declaración de políticas de privacidad y prácticas del DNS (DPPPS). Esta última ayudará a los operadores a preparar sus propias DPPPS. La última llamada del Grupo de Trabajo está a la vuelta de la esquina. En lugar de esperar políticas adicionales, por ejemplo, para que se establezca el DoH, los autores pretenden mantener vivo el documento con incorporaciones y cambios que se consideren regularmente. Los autores piensan que esperar a que los proveedores de DoH formulen políticas como la Política de servidor de confianza de Mozilla demoraría la producción del *draft* innecesariamente.

El tema principal para DPRIVE (tras la publicación del DNS sobre TLS [DoT]) ha sido asegurar el próximo paso, de resolutor a servidor autoritativo. En lugar de los posibles próximos pasos en ese sentido, Tim April (Akamai) presentó muy brevemente un *draft* (que escribió junto con Jason Livingood, Comcast, y Karl Henderson, Verisign) sobre los problemas operativos con el DoT para servidores autoritativos (ADoT). Las preocupaciones incluyen problemas de desempeño, como el "efecto secundario no deseado" de borrar la señalización de EDSN0 Client Submet (ECS) o la necesidad de que un resolutor "pruebe" si un servidor autoritativo estará listo para el DoT. Si bien Tim April remarcó que el documento no era sobre los motivos para usar ADoT, sino sobre las preocupaciones que deben sopesar aquellos que lo implementen, el *draft* hace la siguiente declaración: "En los niveles más altos, se puede argumentar que las técnicas como la minimización de QNAME y el uso agresivo del caché validado por DNSSEC (RFC8198) brindan un camino alternativo hacia la mitigación de los riesgos de divulgación de información sensible sin el riesgo operativo del cifrado del DNS". El *draft* también señala problemas de monitoreo y, originalmente, hizo referencia al altamente controversial *draft* de Matthew Green sobre las claves estáticas en TLS para permitir intercepciones en los bordes de la red.

Otros cuatro documentos se tomaron en consideración en DPRIVE, dos de los cuales están relacionados con los problemas de implementación de DoT y DoH, y dos más que apuntan al abordaje del problema de las transferencias de zona en texto claro.

Un documento que preparó Alessandro Ghedini de Cloudflare aborda la potencial filtración de datos al enviar los llamados datos preliminares en las implementaciones de DoT. El TLS 1.3 permite enviar datos antes de que se complete el *handshake* del TLS. Aunque guarda un viaje de ida y vuelta para completar el *handshake*, esto permite que un potencial atacante extraiga información sobre estas consultas. El documento propone técnicas de mitigación, pero aún debe profundizarse.

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

Otro documento que presentó en Montreal Michael Richardson (Sandelman Software Works), junto con Tirumaleswar Reddy (McAfee), Dan Wing (Citrix Systems) y Mohamed Boucadair (Orange) brinda mecanismos para ejecutar en tiempo de *boot* (bootstrap) los extremos para descubrir y autenticar los servidores DoT y DoH locales. Tiene el propósito de permitir que los empleados que lleven sus dispositivos descubran y autentiquen el servidor para su resolución DNS. Según Richardson, otro caso de uso sería para los entornos de IoT.

A continuación, se puede ver un pantallazo del mecanismo.

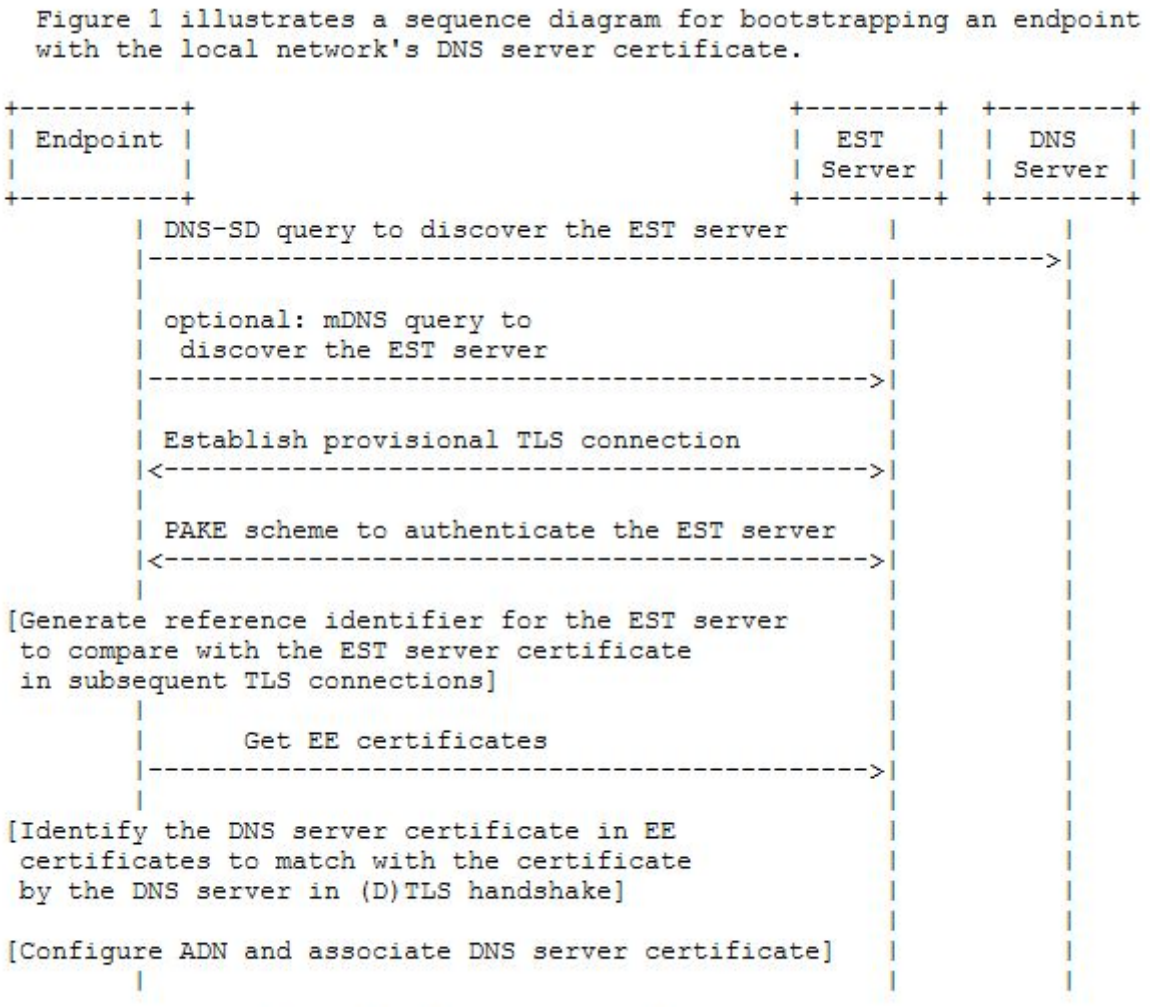


Figure 1: Bootstrapping Endpoint Devices

Se evitó un debate altamente controversial durante DPRIVE en una de las dos propuestas sobre el tema de asegurar las transferencias de zona

Según el primero de los dos *drafts* (DNS Zone Transfers over TLS), las transferencias de zona AXFR se llevan a cabo regularmente sobre el TCP; por lo tanto, cifrar AXFR usando DNS sobre

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

TLS era sencillo. Además de AXFR (usando el TCP), el *draft* también aborda IXFR, que permite tanto el UDP como el TCP. Las implementaciones ya existen en Unbound versión 1.9.2, por lo que, según algunos participantes, el *draft* documenta una práctica actual. Durante la Hackatón de la reunión IETF105, se codificó el soporte XOT para la biblioteca DNSjava. Si bien hay varias preguntas, por ejemplo, con respecto a la necesidad de hacer obligatorio el TLS 1.3 (en lugar de versiones anteriores del TLS) o si es necesario el relleno (*padding*), los participantes del Grupo de Trabajo recibieron el *draft* con gusto, al parecer.

El segundo *draft* no fue bien recibido. Incorpora las operaciones DNS con cortafuegos *stateful* a fin de asegurar las transferencias de zona sin la necesidad de interacciones de notificación ("notify") y SOA por adelantado. El mecanismo parece algo complicado, y no solo para quienes son ajenos a este. Un participante en la reunión lo describió como una "mezcla rara de cosas". Petr Špaček de CZ.NIC se opuso fervientemente al concepto. Otros también expresaron que el Grupo de Trabajo de DPRIVE no era el correcto para este tema, así que los presidentes del Grupo tomarán una decisión sobre qué hacer con la propuesta, que podría incluir enviarla al Grupo de DNSOP.

BoF sobre LAKE, MOPS y obstáculos en la inclusión de los nuevos participantes

Una vez más, varias BoF ilustraron el interés del IETF en integrar tanto la nueva tecnología como los nuevos grupos de participantes, y, a la vez, tomar una postura conservadora en cómo lograrlo, mostrando una preferencia por la serie de estándares del IETF en lugar de estándares alternativos.

Por ejemplo, en la BoF de LAKE (intercambio de claves autenticadas livianas), comenzó un debate sobre si un nuevo protocolo de intercambio de claves similar al TLS podría encajar mejor con la creciente cantidad de entornos de IoT o si un derivado del TLS 1.3 podría llevar a cabo esta tarea. Göran Zelander (Ericsson) propuso Ephemeral Diffie-Helman over Cos (EDHEC), argumentando que EDHEC podría agregar secreto perfecto hacia adelante al recientemente estandarizado Object Security for Constrained Devices (OSCORE).

Durante la sesión, el exdirector de área del Área de Seguridad, Erik Rescorla (Mozilla), ofreció, en cambio, una pequeña versión del TLS 1.3, argumentando que el IETF había dedicado mucho esfuerzo y tiempo en el desarrollo del TLS 1.3 y que sus propiedades de seguridad estaban bien probadas. Al mismo tiempo, dijo que había muchas generalidades que se podrían eliminar de la versión completa, especialmente el valor predeterminado de configuración y la evasión de las negociaciones de versiones para el TLS 1.3.

Al final, la BoF se dividió en dos bandos respecto de qué camino seguir. Algunos participantes como Elliot Lear advirtieron en contra de no elegir un candidato, habiendo tenido la experiencia de decisiones demoradas en Grupos de Trabajo como TCPINC hace algún tiempo. Otros defendían la posibilidad de que se desarrollen ambas soluciones, argumentando que CTLS y EDHEC tenían diferentes características, y que CTLS posiblemente demandaría muchos recursos para los nodos de IoT.

Otro ejemplo de cruce de palabras se observó en la BoF de Operaciones de Medios (MOPS). Glen Deen (ComcastNBC Universal) observó que los expertos en video a veces tenían problemas operativos con las RFC del IETF, de las que dependen fuertemente las series de

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

estándares como SMTPE 2110. SMTPE 2110 define el uso de las redes IP para la producción profesional de video. Los defensores de MOPS, por lo tanto, pidieron un lugar en el IETF donde pudieran evacuar sus preguntas e inquietudes operativas. Si bien los defensores de la BoF presentaron un *draft* de taxonomía para ilustrar la necesidad de un mejor entendimiento y cooperación entre las dos esferas, los veteranos del IETF dijeron que la idea de simplemente crear tal espacio para una comunidad específica no se alineaba con las modalidades usuales de Grupo de Trabajo del IETF. En lo que se podría considerar como un intento para ser como el IETF, los impulsores presentaron un documento sobre taxonomía.

Otro grupo más está lidiando con las políticas del IETF/IRTF. Una vez más, el grupo de Investigación de Detención de Malware e Investigación de Amenazas (SMART) se reunió en sesiones paralelas. El grupo quiere formular su carta constitutiva como un Grupo de IRTF, pero sus propuestas, hasta ahora, parecen incluir la misma cantidad de trabajo en protocolo que en investigación, según Colin Perkins, presidente del IRTF. Un interés original del grupo es trabajar en las consecuencias del cifrado para el monitoreo, incluso con ese tema en particular eliminado de la carta constitutiva. Si el grupo logra formular su carta constitutiva, estará abierto. En una segunda reunión paralela, se debatieron los documentos en la agenda del grupo, sobre Capacidades y limitaciones de una solución de seguridad solo en el extremo (CLESS) y —al igual que en el grupo de MOPS— sobre un documento de taxonomía relacionado. Se podrían considerar otros caminos para incorporar estos documentos en el proceso del IETF/IRTF.

Parece haber un dilema fundamental en el IETF: ¿debería recibir nuevos grupos, especialmente como los dos últimos, para intentar presentarse como abierto (y, así, promover una concurrencia mayor) o podría suceder que estos esfuerzos desdibujen el mandato original del IETF?

La reunión IETF106 tendrá lugar en Singapur del 16 al 22 de noviembre de 2019.

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