Informe de CENTR IETF 101

Londres, 17 - 23 marzo de 2018

Traducción - LACTLD

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

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

LACTLD
Latin American and Caribbean ccTLDs Organization

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

Aspectos destacados

La lucha sobre el cifrado en TLS

Continúa la lucha de poder sobre el cifrado en el IETF. Tuvo lugar un debate digno de mención en el Grupo de Trabajo (WG) de TLS en Londres, que luchó sobre otra propuesta presentada por Russ Housely, antiguo presidente del IETF, para un grupo de negocios de EE. UU.: bancos, concretamente.

LOS CAMBIOS DE 1.2 A 1.3

La especificación de TLS 1.3 básica ya está en camino hacia la edición de RFC, lo que significa que el Grupo Directivo de Ingeniería de Internet (IESG) ya aprobó el *draft*. Un cambio importante en el TLS 1.2 es la decisión de que algoritmos de cifrado modernos se ubiquen en una más rápida y más segura criptografía curva elíptica (ed25519 y ed448). Las suites de cifrado Static RSA y Diffie-Helman han sido eliminadas. El *draft* RFC promete secreto perfecto hacia adelante. Los mecanismos de autenticación e intercambio de claves también fueron separados del algoritmo de protección de registro para defenderse mejor ante ataques activos. Para acelerar el protocolo, se añadió un modo 0-RTT, lo que permite comenzar el intercambio de datos con el primer paquete, a costas de algunas propiedades de seguridad.

Una de las características más importantes de TLS 1.3, ciertamente, es que la mayoría de las partes del encabezado ahora están cifradas. Luego del ServerHello, todos los mensajes handshake están cifrados. El mensaje de extensiones cifradas también permite que las extensiones sean enviadas a salvo antes de ser cifradas.

ACTORES ESTATALES Y DE LA INDUSTRIA MUESTRAN PREOCUPACIONES ACERCA DE QUEDAR A OSCURAS

El foco de acalorados debates en el IETF es el hecho de prever un grado más alto de confidencialidad de extremo a extremo. Varios operadores de centros de datos, el sector bancario de los EE. UU., y también el Centro de Ciberseguridad nacional británico (NCSC, por sus siglas en inglés) tomaron un rol activo durante la sesión de TLS 1.3 en Londres. Advirtieron sobre los efectos negativos del cifrado de extremo a extremo en TLS 1.3.

El NCSC había presentado una advertencia apenas una semana antes de la reunión del IETF en Londres, que indica que ganaría la seguridad individual, pero la seguridad empresarial perdería, debido a que el monitoreo, el filtrado y la resolución de problemas serían mucho más difíciles de llevar a cabo.

Un *draft* presentado individualmente por la recientemente establecida organización de Operadores de Centros de Datos Empresariales explica el razonamiento de aquellos que instan a una solución de inspección:

«*Hoy en día hay empresas con redes extensivas de brókeres de paquetes que están llevando a cabo el descifrado fuera de banda de TLS para alimentar a los husmeadores de la red, dispositivos de detección de intrusión, detección de fraude, detección de malware, herramientas*

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

de monitoreo de desempeño de aplicación, herramientas de monitoreo de la experiencia del consumidor, y otras soluciones. Hace 20 años que existe la capacidad de realizar el descifrado fuera de banda, y por primera vez en la historia, desaparecerá con el traspaso a TLS1.3 [TLS13]».

La lista de problemas que debieron abordar los operadores de red incluye ataques DDoS, monitoreo de fraude, monitoreo de detección de intrusión, detección de amenazas y respuestas a incidentes. Las alternativas que incluyen el descifrado de hombre en el medio dentro de la red, el uso de encabezados TCP o UDP, el seguir utilizando TLS 1.2, y el registro, seguridad y resolución de problemas en el extremo, la inspección de tráfico cifrado o Ipsec se consideran muy riesgosas, muy costosas, o sin la suficiente granularidad. Implementar proxies en su lugar costaría millones, según dijo a quien escribe Russ Housley, antiguo presidente del IETF. Los requisitos regulatorios citados hasta el momento están muy limitados a la regulación de los EE. UU. contra el tráfico de información privilegiada.

UNA SOLUCIÓN *OPT-IN* PARA LA «VISIBILIDAD»

Debido a que una propuesta original para prever una clave estática Diffie-Helman para el descifrado por parte de administradores de centros de datos no logró llegar a un consenso el año pasado, la comunidad bancaria de los EE. UU. en Londres regresó con una propuesta para prever un mecanismo *opt-in* que deje entrar un número más pequeño de puntos del centro de datos dentro del tráfico.

Presentada por el expresidente del IETF, Russ Housley, la «extensión a TLS1.3» propuesta restringe la inspección a los casos en los que un cliente señale el conocimiento a ser inspeccionado en el *ClientHello* y luego reciba claves efímeras para la sesión. Housley indicó que «no se compartirán claves privadas». Un segundo conjunto de claves distribuidas de antemano por el gestor de claves en el centro de datos limitaría los destinos con los que se compartirían los paquetes descifrados.

Housley resaltó las ventajas: transparencia para el cliente y mejor seguridad en el centro de datos durante los tiempos inactivos, o los ataques contra el tráfico descifrado. Sin embargo, admitió que el mecanismo no estaba limitado a los centros de datos. Si bien los clientes normalmente actúan como balanceadores de carga en el límite del centro de datos, también podrían ser terminales de pago por fuera.

EL IETF RECHAZA LAS SOLUCIONES *OPT-IN* EN UNA SESIÓN TECNO-THRILLER

La sesión del IETF que decidió sobre el *draft* de Housley no fue nada menos que un pequeño thriller tecnológico. Los opositores decididos, en particular el exdirector del área de seguridad Stephen Farrell, cuestionaron el procedimiento de agregar una propuesta más a la agenda del WG. El presidente del IAB, Ted Hardie, le recordó al grupo que había un número de actores estatales que podrían obligar a los operadores de su región a brindar la información de clave correspondiente, también para la futura inspección del tráfico.

Por lo tanto, un enfoque «voluntario» todavía representaba una debilidad en la arquitectura. La historia y Snowden nos han demostrado que los operadores de centros de datos y los actores

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

estatales no siempre están de acuerdo en lo que significa la privacidad, según explicó Hardie, refiriéndose a la vigilancia del tráfico de centros de datos entre los centros de datos de Google descifrados. Por ello, ocultar las claves a terceros poderosos era improbable. Los opositores también hicieron referencia a las alternativas técnicas disponibles.

Varios intentos de la directora de área de seguridad saliente, Kathleen Moriarty, para la construcción de puentes con limitaciones adicionales a la solución presentada por Russ Housley, fueron rechazados por este último por no ser suficientes.

Al final, la votación informal que los presidentes del WG decidieron tomar reveló que los centros de datos/trincheras de seguridad estatal habían enviado lo mejor de ellos para completar las filas. El NCSC había traído a cuatro, y el Banco de EE. UU. había llevado, por su parte, a 14 personas. La postura que favorecía la adopción del *draft* de visibilidad era claramente tan fuerte como la que estaba en contra. Un participante que estaba sentado cerca de la «facción» de centro de datos observó, a modo de broma, que era claro que habían hecho ejercicios de respiración antes de la sesión.

Finalmente, los presidentes del WG decidieron que no había consenso para adoptar la propuesta.

REACCIONES Y PASOS POR SEGUIR

Luego de la sesión, Housley le dijo a quien escribe que no esperaba que la comunidad de los centros de datos renunciara a sus propuestas, pero que sus integrantes no volverían al IETF. En cambio, indicó que el ETSI (Instituto Europeo de Estándares de Telecomunicaciones) estaría feliz de intervenir y que esperaba que los representantes de los centros de datos asistieran. Lo mismo había sucedido para el estándar de interceptación legal hace más de una década. La desventaja, desde el punto de vista de los defensores de la privacidad, era que en lugar de una solución *opt-in* más transparente, el ETSI podría estandarizar la solución de clave original estática Diffie-Helman (*draft*-Green).

Quic: La lucha sobre un *Spin Bit*

Más discusión tuvo lugar con respecto a la inspección del tráfico durante la reunión del WG de Quic, pero en un nivel diferente. Mientras que la trinchera de los centros de datos está pidiendo, para TLS, los textos claros de los paquetes, en Quic, los operadores de la red están buscando información sobre los metadatos. Esperan al menos un solo bit, el «*spin bit*», para medir los viajes de ida y vuelta y llevar a cabo la resolución de problemas.

El emergente protocolo de transporte originado en el laboratorio de Google, que está basado en UDP, es mucho más estricto con el cifrado de los metadatos. «A diferencia del TCP, la imagen en el cable de Quic expone mucha menos información sobre el estado del protocolo de transporte que la imagen en el cable del TCP», explica el *draft* sobre *spin bit*. Especialmente, perder los números de secuencia y reconocimiento además de los sellos de tiempo (disponibles en el TCP) hace que sean imposibles las mediciones pasivas en el camino.

Como en TLS, tuvo lugar un considerable debate entre los 200 participantes por más de 90 minutos. Al final, no se rechazó por completo la inclusión de la solución *spin bit* para las

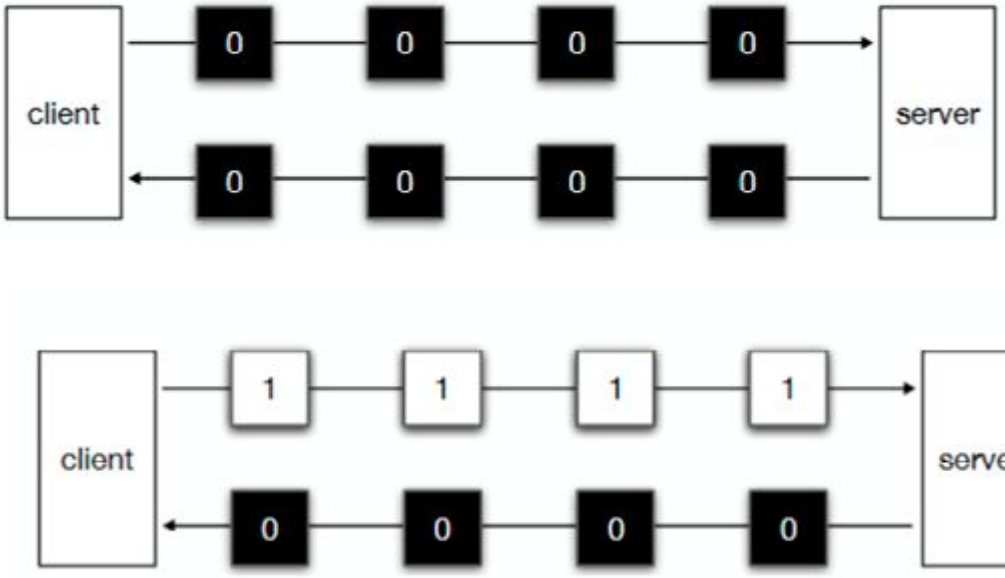
Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

mediciones pasivas de los tiempos de viaje de ida y vuelta, pero se la dejó de lado por ahora para terminar primero la versión 1 de Quic.

SOLO UN *BIT*

Brian Trammell, académico en ETH Zurich y miembro de la Junta de Arquitectura de Internet, presentó en Londres la propuesta del *draft* del *spin bit*. La lista de coautores (Huawai, Telecom Italia, Nokia, Ericsson y AT&T Labs) demuestra el interés de los operadores de redes, operadores de telefonía móvil, y proveedoras de red.

Básicamente, el mecanismo consiste en un solo *bit* añadido a la parte del texto puro del encabezado. Será configurado a cero por el Cliente y modificado a uno cuando la respuesta llegue al cliente (un viaje de ida y vuelta, vea el gráfico). El «cambio» permite la medición pasiva de tiempo de viaje de ida y vuelta por un observador externo, y, según Trammell, es de peso liviano y también fácil de implementar.



Trammell admitió, durante su presentación, que el RTT podría estar un poco sobrevalorado por los mecanismos con flujos de red imperfectos, pero que eliminar ciertos efectos ayudaría. Con respecto a la privacidad, un grupo de diseño, al que Tom Hardie representó para informar al WG, no había encontrado problemas con la solución *spin-bit*, al menos siempre y cuando el *spin bit* sea realmente un solo *bit*. Trammell aclaró que una solución de dos *bits* mejoraría la confiabilidad, pero que eso no era parte de lo que proponía el *draft*.

Las soluciones con *spin bit* fueron implementadas en MINC y Quic-Go durante el Hackaton de IETF, según informó Trammell.

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

SPIN BIT UBICADO EN UNA VÍA LATERAL

Aunque no hubo candidatos para las «invariantes» del protocolo Quic según el consenso en el WG de Quic, la propuesta del *spin bit* estuvo muy cerca de ser incorporada en la versión 1 de Quic. Miriam Kuehne, directora del Área de Transporte, e investigadora en ETH, argumentó a favor de incluirlo, para ganar experiencia con el *spin bit*.

Incluso algunos guardianes de la privacidad, como Daniel Kahn Gillmore, de la Unión Americana de Libertades Civiles, pareció ceder a causa de la evaluación positiva de la compatibilidad con la privacidad.

Al final, las preocupaciones que resultaron en el aplazamiento de la última llamada se originaron a partir de preocupaciones técnicas y del proceso de salida al mercado para el documento estándar.

SPIN BIT: LOS EFECTOS Y LA INDISPENSABILIDAD NO ESTÁN LO SUFICIENTEMENTE CLAROS

El editor de Quic, Jana Iyengar (que acaba de trasladarse de Google a Fastly), advirtió que incorporar el *spin bit* en la versión uno podría demorar la finalización de la versión 1 de las especificaciones, que ha sido levemente pospuesta a noviembre de 2018. Remarcó que no estaban completamente claros los efectos de añadir el *spin bit* al encabezado abierto. Sobre la privacidad, Iyengar dijo que, a pesar de que el *spin bit* parecía pasar desapercibido, a veces se encuentran problemas de privacidad más adelante. No obstante, Iyengar criticó a las operadoras de red. No lograron aclarar por qué y cómo el *spin bit* era indispensable para la administración de la red.

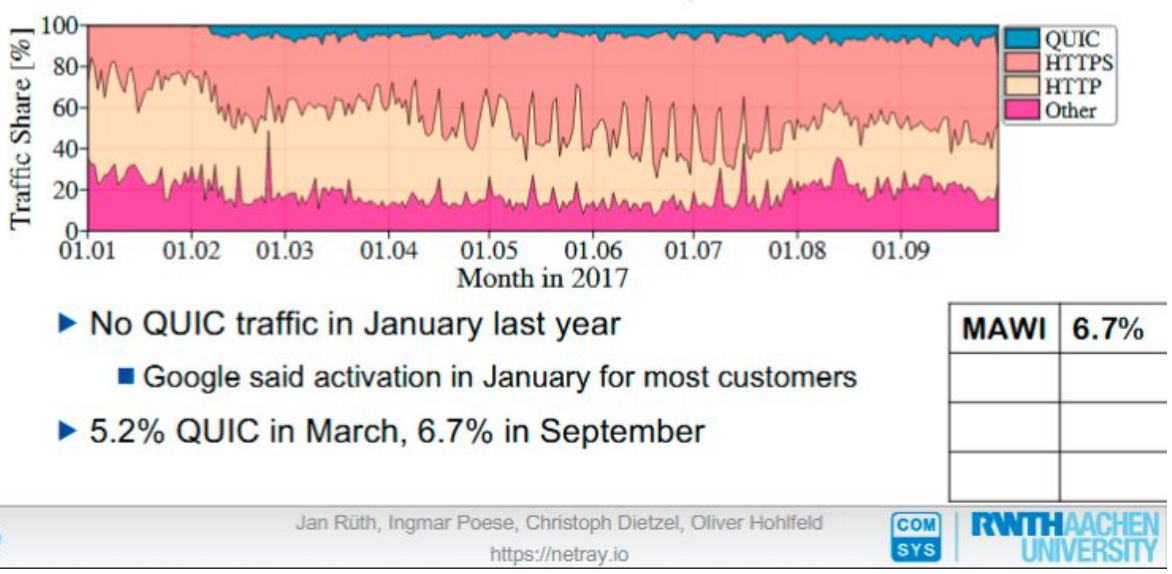
¿Existirán para Quic debates similares a los de TLS sobre los metadatos cifrados? Iyengar dice que es posible. Aun así, para el contenido, se enviaría a las personas a TLS. Quic solamente podría volverse el blanco de debates sobre metadatos.

STATUS QUO DE QUIC

Mientras tanto, las mediciones pusieron el tráfico de Quic al 9 o 10 por ciento. Prácticamente todo es tráfico de Google, y más del 40 por ciento del tráfico de Google ahora viaja por Quic, según Iyengar. Akamai también implementó a Quic, pero el tráfico de Quic en Akamai todavía era «insignificante», potencialmente debido a que los clientes de Akamai deben decidir voluntariamente usar Quic. Se presentaron más cifras detalladas sobre el tráfico de Quic en la sesión del Grupo de Investigación de Evaluación y Análisis de Protocolos (MAPRG, por sus siglas en inglés).

Iyengar admitió que era un proyecto ambicioso lograr que Quic esté finalizado para la reunión IETF en Bangkok. El gran problema por resolver durante los próximos meses (se llevará a cabo otra reunión interina en Estocolmo) está relacionado con el *handshake*.

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



La lucha sobre el cifrado a lo largo de la pila

Los debates de TLS y Quic sobre los efectos del cifrado son claras expresiones de una permanente lucha de poder. Con el cifrado, le explicó un ingeniero a quien escribe, el poder queda expuesto en un lugar. Los cambios en TLS y Quic actualmente resultan en un cambio de dónde se ubican las claves. Aquellos que antes tenían acceso al tráfico de texto puro o de metadatos son excluidos con el tráfico TLS añadido, mientras que los proveedores de aplicaciones siguen funcionando con el usuario en el extremo. Según el ingeniero, el cambio de poder explica la ferocidad de los debates.

Además, los actores estatales ven el cambio como algo conflictivo con sus objetivos. Un funcionario del NCSC, mientras hablaba con quien escribe tras la votación, señaló que la oficina esperaba rebuscárselas cuando fuera necesario. Curiosamente, Sujit Raman, procurador general adjunto y socio en el Departamento de Justicia, durante la cumbre Global Privacy el 27 de marzo en Washington, hizo referencia al cifrado añadido en los protocolos y advirtió que estaba mal dejar que solo los tecnólogos tomen las decisiones sobre el cifrado

En el IETF, el debate toma forma en muchos lugares. Además de los debates sobre TLS y Quic, también existieron los siguientes:

- Una presentación de un grupo de ingenieros de Cisco (dirigida por Nancy Cam-Winget) que halló la forma de hacerse lugar en el WG de OPSEC sobre «El impacto de TLS 1.3 sobre la seguridad basada en la red», en la que explicaron: «*TLS 1.3 indica que el cliente DEBERÍA incluir una extensión "key_share" para habilitar que el servidor decline la reanudación y recaiga en un handshake completo, aunque este no es un requisito absoluto. Algunas situaciones ejemplificativas que sufrirían el impacto de esto son las middleboxes que no son parte del handshake inicial, y por lo tanto no conocen la PSK. Si el cliente no incluye la extensión "key_share", la middlebox no puede forzar un regreso al*

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

handshake completo. Si la política de middlebox le exige inspeccionar la sesión, tendrá que en cambio causar un fallo de conexión».

- Existe un *draft* individual de Gory Fairhurst (Universidad de Aberdeen) y Charlie Perkins (Universidad de Glasgow) sobre «El impacto del cifrado de encabezado de transporte sobre el funcionamiento y la evolución de la Internet», que recibió críticas en la lista de correos de Opsec por incluir oraciones como:
«*El uso generalizado del cifrado del encabezado de transporte puede impactar las maneras en que los protocolos se diseñan, se estandarizan, se emplean, y se operan. Por lo tanto, la decisión de que los futuros protocolos de transporte cifren sus encabezados de protocolo necesita evaluarse no solamente desde el punto de vista de la seguridad y la privacidad, sino también desde el impacto en el funcionamiento, los estándares, y la investigación*».

- Durante la sesión plenaria, Stephane Bortzmeyer (Afnic) se opuso una vez más a llevar el documento sobre «Los efectos del cifrado generalizado en los operadores» desde la directora del Área de Seguridad, Kathleen Moriarty, al editor de la RFC. Bortzmeyer argumentó durante el debate con los miembros del IESG que habían autorizado el documento, que el IETF debía tomar una posición del lado de la privacidad. La propuesta de «neutralidad» en lo que se conoció como la «lucha» entre la privacidad individual y la seguridad de los operadores fue falsa.

Experto en DNS alerta: no hay que sobrecargar el «Camello»

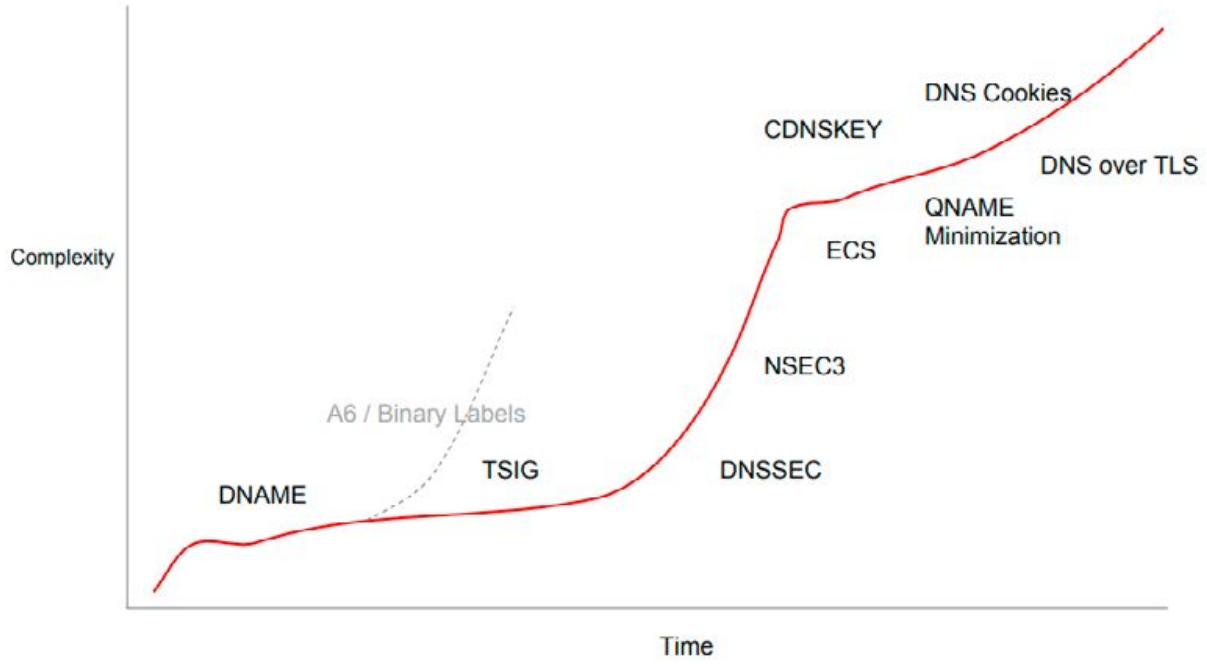
Hay 185 RFC, 2.781 páginas y 888.233 palabras: todo eso es el DNS y es demasiado para el viejo, trabajador y confiable protocolo, señaló Bert Hubert, de PowerDNS en una presentación sobre el «Camello» del DNS. De una manera muy entretenida, Hubert quiso hacer referencia a lo que él considera un problema grave: la creciente complejidad y el exceso de ingeniería del protocolo. La sesión del DNS en Londres fue un ejemplo de este problema, según mencionaron algunos expertos en el tema. Tim Wicinski dijo que, actualmente, el WG tenía 14 documentos en varias etapas del proceso RFC (vea el informe del WG más abajo), y que había más en camino —y que los dos copresidentes pedían un tercero para compartir la carga de trabajo.

COMPLEJIDAD: RIESGOS DE FALLAS Y CONSOLIDACIÓN EN EL MERCADO

Según Hubert, las DNSSEC fueron el momento decisivo, en el que la complejidad introducida en el DNS comenzó a resultar prohibitiva para los actores más pequeños. Dos proveedores de DNS pequeños pero bien establecidos, MyDNS y DNS Mara, cerraron sus negocios por ser incapaces de seguir el ritmo de implementación de la tecnología del DNS cuando se introdujeron las DNSSEC.

Luego de las DNSSEC, se estandarizaron el NSEC, NSEC3, Qname Minimization, CDNSKey, DNS sobre TLS, y la lista no termina ahí.

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



El creciente número de estándares incrementó la complejidad del DNS. Esto hizo que las operaciones fueran más propensas a fallas, especialmente porque a menudo el personal en las operaciones del DNS era insuficiente. Una compañía como Comcast tenía 21 expertos en DNS. «Esa cantidad iguala a la cantidad de todos mis clientes juntos», dijo Hubert sobre los clientes de PowerDNS. Otro resultado fue la tendencia a recurrir a las grandes compañías de DNS. Estos grandes proveedores también trajeron un nuevo trabajo en estándares, diseñados especialmente para sus necesidades para con el IETF, lo que se sumó a la lista.

Según Hubert, una particularidad del DNS era que, a diferencia de otras áreas del protocolo, había mucho software de código abierto, que era muy bueno e incluso gratis (Bind, NLnetlabs, Knot). De igual manera, los programadores y autores de estándares fueron muy inteligentes y siempre estaban ajustando los estándares, incrementando así la complejidad en el tema. Además, no hubo resistencia al desenfreno de la estandarización. Los implementadores del DNS que no son parte del grupo cerrado de autores de estándares/implementadores no se animaron en el IETF a decir que las nuevas RFC les resultaban muy complicadas y difíciles de implementar. Los operadores no participaron en el IETF para actuar como correctivo.

Las reacciones del WG de DNSOP fueron diversas. Desde la defensa absoluta para permitir que el DNS se extendiera y se usara de nuevas formas (Alain Durand, ICANN) o el mero reconocimiento de que el hecho de que el DNS fuera un «gran éxito» sería la causa de su uso de «maneras impredecibles» (Andrew Sullivan, Oracle) hasta consideraciones sobre la redacción de más documentos que expliquen por qué fueron creadas las extensiones (Matthijs Mekking). Representantes de CZ.NIC señalaron que ellos habían comenzado a abordar el problema de los métodos alternativos al EDNS (RFC6891). Vea su comunicado de prensa. También surgieron preguntas fundamentales. John Klensin propuso poner un freno temporal a los nuevos

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

estándares para aprovechar el tiempo y preparar un documento de supervisión con fines orientativos. En una RFC informativa publicada recientemente, Klensin pidió que se debata la necesidad del DNS de reducirse, reformarse o desarrollar la v2.0 (RFC 8324).

RegEXT – Extensión para las políticas de contratación de ICANN

En el WG de Extensión de Registro de la reunión IETF101 se desarrolló un debate tras el anuncio de que se prepararán nuevas extensiones de registro en ICANN. Jim Galvin (Afilias), presidente del WG de RegExt, observó que los registradores no tenían buena representación en el IETF, y que el grupo de RegExt era un WG algo pequeño. Por lo tanto, estimó que las propuestas presentadas por los registradores en ICANN podrían llegar al IETF. Tanto el subcomité del registrador TechOps y el grupo TechOps en los registros como también un grupo conjunto podrían ser fuentes. Galvin dijo que había varios documentos en camino desde el subcomité del registrador TechOps hacia el proceso de estandarización (sobre nombres no disponibles, formatos de archivo para informes entre registros y registradores, y formato de archivo de transacciones de facturación).

Alexander Mayrhofer, nic.at, que ha sido uno de los revisores de las extensiones pendientes, se pronunció en contra de permitir que actividades que establezcan estándares se lleven a cabo por fuera del IETF, y que se use al IETF solo para conseguir su sello. Estaba preocupado por el hecho de que los grupos TechOps de ICANN eran exclusivos para miembros, lo que significaba que los trabajos sobre estándares se realizaban en espacios cerrados.

Además del aspecto procesal, algunos de los mecanismos a los que se refirió Galvin parecían aspectos más organizacionales (o incluso contractuales), en lugar de problemas técnicos. Una RFC, especialmente una que pretenda llegar a «*standard*», podría ser demasiado.

Galvin argumentó que sería mejor traer el trabajo correspondiente al único lugar en el WG de RegExt del IETF, en lugar de llevarlo a cualquier otro sitio. Los más escépticos imaginan un uso estratégico del proceso, incluso con posibles mecanismos contractuales que se conviertan en «estándares» y se consideran obligatorios por esa razón. Un documento administrativo, por ejemplo, es el *draft* actualmente estancado de la oficina de ICANN sobre la especificación funcional de «Trade Mark Clearing House».

MUCHO QUE PROCESAR Y POCOS REVISORES

Hace tiempo que es preocupante que el WG tenga una membresía tan limitada y que los documentos no se examinen con minuciosidad como lo hacen otros WG del IETF. Hasta el momento, VeriSign ha traído muchas propuestas y, en menor medida, también los registros ccTLD como SIDN y CNNIC. El único registrador activo en el grupo hasta ahora ha sido GoDaddy.

Las tres RFC que el WG ya dio por finalizadas son:

- RFC 8056: Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol Status Mapping (VeriSign) («mapeo entre EPP y RDAP»)

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

- RFC 8063: Key Relay Mapping for the Extensible Provisioning Protocol (SIDN) («envío de llaves DNSSEC por dentro de EPP») (existe una declaración de derechos de propiedad intelectual aparentemente poco problemática de VeriSign sobre este mecanismo)

- RFC 8334: Launch Phase Mapping for the Extensible Provisioning Protocol (VeriSign, CentralNic, Cloud Registry) («soporte dentro de EPP para las fases de lanzamiento de nuevos TLDs»), y la antigua RFC 7848 sobre los procedimientos de lanzamiento con marcas registradas («Sunrise trademark»), Mark and Signed Mark Objects Mapping (ICANN)

El WG está a punto de reformular su acta constitutiva para tomar nuevos trabajos, con bastantes documentos todavía en proceso, y que todavía necesitan revisión. La lista incluye:

- Verification Code Extension for the Extensible Provisioning Protocol (VeriSign)
- Validate Mapping for the Extensible Provisioning Protocol (GoDaddy)
- Registration Data Access Protocol (RDAP) Object Tagging (VeriSign, Arin)
- Organization Extension for the Extensible Provisioning Protocol, el *draft* del exdistribuidor (CNNIC)
- Extensible Provisioning Protocol (EPP) Organization Mapping (CNNIC)
- Registry Fee Extension for the Extensible Provisioning Protocol (GoDaddy, CentralNic)
- Third Party DNS operator to Registrars/Registries Protocol (CIRA, Red Hat) Change Poll Extension for the Extensible Provisioning Protocol (EPP) (GoDaddy)
- Bundling Domains (CNNIC)
- Allocation Token Extension for the Extensible Provisioning Protocol (VeriSign)

Puede ver la lista completa de documentos (hitos) aquí. Los nuevos trabajos incluyen un gran número de extensiones relacionadas con el RDAP para la búsqueda, la búsqueda inversa, el acceso federado y demás.

WHOIS DESCENTRALIZADO: OTRA PROPUESTA DE CENTRALNIC

Con el RGPD (nuevo reglamento de privacidad europeo) como cuestión principal para los registros y registradores, Gavin Brown (CentralNic) propuso hacer el intento de descentralizar Whois. Presentó Whoiam como una alternativa descentralizada que consistiría en Whois ligero combinado con la publicación de datos de la v-card publicada por el dueño de un dominio (y propuso que también podría incorporarse directamente en el DNS). Los registrantes podrían tomar el control de la publicación de sus datos (o terciarizarlo, si lo prefieren, inclusive a *proxies* privados). También serían capaces de verificar quién accedió a la información, lo que incrementa la transparencia.

Los registradores y los registros cederían la responsabilidad a los registrantes y se beneficiarían al no ser los encargados de publicar y controlar el acceso a terceros. Si bien Brown dijo que el acceso diferenciado podría llevarse a cabo, también remarcó que la minería de datos sería posible de todas formas.

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

Scott Hollenbeck (VeriSign) consideró imposible hacer cumplir las obligaciones de publicación a los usuarios finales.

El WG todavía no adoptó el documento.

Grupos de trabajo (WG) y grupos de debate informal (BoF)

WG de DPRIVE

El WG de DPRIVE está a punto de reformular su carta constitutiva, ya que se lograron sus hitos con respecto a los mecanismos de privacidad del DNS para el intercambio de datos del DNS entre los resolutores *stub* y los resolutores recursivos (DNS sobre TLS, DNS sobre DTLS, Profiles, Qname Minimization). Otro *draft* sobre rellenado (contra los ataques de análisis de tráfico) pasó la última llamada, y la revisión de seguridad, y se encuentra camino al IESG.

La siguiente cuestión por abordar es el camino desde los servidores de nombres recursivos hasta los autoritativos. A diferencia de la relación bastante estable entre el *stub* y el recursivo, los recursivos se comunican con muchos servidores autoritativos, haciendo de este el problema más difícil. Algunos participantes del IETF dan a entender que la mejor solución para un DNS respetuoso con la privacidad es el DNS sobre HTTPS. Stephane Bortzmeyer (Afnic) presentó el breve *draft* sobre «cifrado y autenticación de la comunicación del DNS de resolutor a autoritativo».

Se propone, una vez más, TLS para el transporte seguro, pero para la autenticación se propone Dane. El servidor autoritativo necesitaría añadir un registro TLSA. Luego, el cliente abriría una conexión TLS y se autenticaría vía DANE (la autenticación DANE podría acelerar el proceso, según el *draft* enviado en la sesión TLS usando una extensión dentro de la cadena). El servidor autoritativo podría separar las consultas de los recursivos dependiendo de si solicitan TLS o no, y enviarlas a diferentes servidores, según Bortzmeyer.

Oficialmente, el WG todavía no adoptó el documento. Aunque Bortzmeyer señaló que el próximo paso estaba previsto en la carta constitutiva original, podría ser necesario reformularla de todos modos. La propuesta borrador de la carta constitutiva incluyó mediciones sobre la adopción de DNSpriv (además de la protección del camino del recursivo al resolutor). Sin embargo, varios participantes lo descartaron por denominarlo una cuestión de investigación que podría ser más del ámbito del IRTF.

PRÁCTICA DE PRIVACIDAD

En el intento de documentar la evolución de las opciones de servicios DNS respetuosos con la privacidad —y también de impulsar su adopción— Sara Dickinson (Sinodun) y varios coautores están elaborando «recomendaciones para los operadores de servicios de privacidad del DNS». Según el coautor Roland van Rijswijk-Deij (surfnet.nl), el *draft* apunta a presentar consideraciones operacionales, políticas y de seguridad para especialistas y también ayudarlos a redactar sus declaraciones de políticas de privacidad del DNS.

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

Además de brindar una visión general sobre las nuevas capacidades de mejora de la privacidad para el DNS, el *draft* también aborda el problema de cómo las prácticas operacionales, por ejemplo el registro de consultas DNS en el resolutor, pueden diseñarse de maneras más o menos respetuosas con la privacidad. El registro y monitoreo (y también la retención de datos) podría reducirse a un mínimo y ser anonimizados, con el acceso a los datos almacenados también al mínimo. Los servicios del DNS de privacidad no deberían, según el documento, rastrear a los usuarios, brindar datos a terceros, ni acumular o vender los datos de consulta.

Al igual que en los debates sobre el transporte y el área de seguridad (TLS y Quic), algunas capacidades para la resolución de problemas podrían retenerse usando la pseudoanonimización (i-cipher, filtros de Bloom). Van Rijswijk-Deij presentó experimentos con una solución de filtros de Bloom (aquí encontrará más investigación) que está actualmente en progreso en surfnet. Los filtros de Bloom fueron diseñados en la década del 70 para indexar grandes bases de datos. Según van Rijswijk-Deji, pueden ser explicados como «una manera estadística de verificar la membresía de un conjunto. Los elementos añadidos al filtro de Bloom sufren pruebas mediante funciones *hash*, y el resultado de estas funciones se utiliza para establecer *bits* en una matriz de *bits*. Los contenidos de esta matriz de *bits* se utilizan luego para verificar la membresía del conjunto».

Los filtros de Bloom «no almacenan nombres de consultas originales» (pero sí los resultados de un conjunto de funciones *hash*) y no son numerables. Las búsquedas solo son posibles cuando uno sabe qué está buscando. Al mezclar consultas de múltiples usuarios en un único filtro, se hace más difícil rastrear a los usuarios.

WG de DNSOP

El debate sobre «Camel» dejó una impresión duradera en el WG de DNSOP, al menos durante el IETF101. Teniendo en cuenta dos sesiones de DNSOP, hubo una rápida sucesión de *drafts*, que tras la charla sobre Camel, se dividieron: Camel-no-Camel. Incluso antes de las charlas, el director de área Warren Kumari (Google) dijo que el WG había tenido éxito en la adopción de documentos, pero no tanto en lograr terminarlos. Suzanne Woolf, copresidente del WG, dijo, como respuesta a Hubert, que no todo lo que les llegara que fuera interesante se convertiría en una RFC. Los *drafts* mencionados, o debatidos brevemente, incluyen los mencionados más abajo.

La copresidente Suzanne Woolf le pidió al WG que comente sobre un posible *draft* sobre .alt TLD, que había sido dejado de lado por un tiempo tras haber sufrido duros debates. Ahora Woolf quiere darle un cierre al asunto.

Paul Hofmann, editor del *draft* de terminología, anunció que estaba a punto de llegar a la última llamada del WG (mediados de abril).

Stuart Cheshire (Apple) presentó el *draft* sesión-señal, en confección desde 2015 y una condición previa, observó Cheshire, para un número de *drafts* en el WG de Descubrimiento de Servicios del DNS (DNSSD).

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

Joe Abley (Afilias) llegó para reanimar el *draft Refuse any* (que también data del 2015 y estuvo inactivo por algún tiempo). Debido a que las consultas ANY en el DNS fueron usadas, por ejemplo, para la amplificación o la minería de registros de recursos, podrían ser necesarias las respuestas pequeñas. El *draft* propone varias respuestas mínimas adicionales para las preguntas ANY. El *draft* llegará pronto a la última llamada del WG.

El *draft* del formato de captura del DNS, presentado por Jim Hague, todavía contiene problemas de derechos de propiedad intelectual. El documento contemplará el almacenamiento y transmisiones eficientes de grandes capturas de paquetes del tráfico del DNS.

Tim Wicinski, copresidente del WG, recomendó resolver este problema y pasar pronto a la fase de la última llamada. El concepto se ha empleado en algunos servidores raíz.

Otro candidato para la última llamada del WG es el centinela de la implementación de la KSK que preverá un mejor monitoreo de la preparación de los resolutores para la implementación de la KSK. Permitirá que un usuario final determine el estado de la clave confiable del resolutor que utilice para sus consultas DNS.

El WG debatió un poco más sobre el tipo de registro de recurso ANAME, que es similar al CNAME pero se limita a las consultas de tipo A o AAAA. Funcionará como alternativa a CNAME (en los casos en el uso de CNAME se vea impedido). El debate principal fue sobre dividir el documento para el lado del autoritativo y del resolutor, pero muchos miembros del WG se opusieron.

Hubo mucho apoyo por parte de los representantes de ICANN (David Conrad) y otros para el documento sobre el mecanismo de inicialización («*bootstrap*») de confianza, presentado por Joe Abley (Afilias). El documento brinda una guía sobre cómo los resolutores de validación pueden determinar un ancla de confianza apropiada para la zona raíz para utilizar en la etapa inicial, o cuando otros mecanismos destinados a permitir la implementación de claves (5011) no estén disponibles. Se habla mucho sobre que la 5011 en general debería ser reemplazada por un mecanismo mejor.

Otros trabajos relacionados con las DNSSEC intentan resolver el problema de las compañías que utilizan diferentes proveedores de DNS para su servicio de DNS autoritativo. El *draft*, presentado en Londres por Shumon Huque (Salesforce) expone varios modelos de cómo emplear las DNSSEC en ese caso.

Algunos pensaron que la paja que rompió la espalda del camello —como dice el refrán inglés— fue el documento XPF presentado por Peter van Dijk (ISC). El *draft* propone una «nueva opción dentro del mecanismo de extensión para el DNS EDNS(0) [RFC6891] que permita que un servidor de DNS reciba la dirección IP original de la fuente del cliente cuando esté suministrada por *proxies* de confianza». Esto resolverá los problemas en que los *proxies* frontales finales o *front end* (para el balanceo de carga, por ejemplo) ocultan la dirección original fuente del cliente al servidor del DNS, haciendo que sea más difícil utilizar ACL, DNS, Response Rate Limiting y otras tecnologías del lado del servidor. El *draft* reconoce que el XPF utilizado incorrectamente podría exponer información interna de la red. Debido a que estaba destinado para el *proxy* del lado del servidor (bajo el mismo control administrativo que los servidores del DNS), no hubo

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

cambios en qué datos privados se podrían compartir. Muchos miembros del WG criticaron el *draft* advirtiendo que no sería bueno que el WG dependiera del buen comportamiento y las buenas intenciones de los actores. El WG también tuvo posturas diferentes acerca de otro documento del ISC, una propuesta para el aprovisionamiento de zona automático. Andrew Sullivan dijo que la propuesta era una «granja de camellos».

Para un resumen más detallado de la sesión del WG de DNS, vea las minutas de Paul Hofmann.

WG de Homenet

El WG de Homenet no parece progresar de manera sustancial. El único documento hito debatido durante la sesión fue el simple documento sobre la arquitectura de la red doméstica. El documento describe la publicación, la resolución de nombres y el descubrimiento en las redes domésticas.

El documento sufrió una reescritura sustancial para aclarar, según Ted Lemon, que no era una arquitectura completa, que no se requería ningún resolutor de servicio completo para responder las consultas de la red doméstica («bastará con un *proxy* siempre y cuando divida las consultas para las zonas locales»). Al utilizar un *proxy* de descubrimiento, las siguientes zonas abordadas de manera local serían compatibles:

home.arpa

fc.ip6.arpa

10.in-addr.arpa

168.192.in-addr.arpa

16.172.in-addr.arpa

Las consultas para todas las otras zonas serían respondidas localmente.

Lemon dijo que lo implementaría en OpenWRT y Turris y volvería con código.

La delegación home.arpa, elegida tras descartar la delegación de nombre especial .home, está estancada en la lista de espera del editor de RFC, debido a que la IANA ya completó la delegación. En un debate en la lista de mail de DNSOP, Kim Davis (IANA) explicó que la delegación de home.arpa a AS112 fue elegida como «el mejor enfoque a corto plazo». Aunque tiene «sus propias dificultades», se prefirió tener registros DNAME en los servidores raíz para la delegación insegura necesaria de home.arpa. La delegación insegura de las DNSSEC es necesaria para que los resolutores de validación/enrutadores domésticos no bloqueen la resolución de home.arpa.

La seguridad perimetral para la red doméstica se debatió brevemente. Este asunto, si bien es un hito, ha estado inactivo y el presidente del WG dijo que si no había nada inminente, daría por cerrado el asunto. Ted Lemon señaló que sería capaz de trabajar en este asunto entre el IETF 101 y el 102. Se debatió brevemente la seguridad para babel (ya sea mediante hmac o DTLS).

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

En un intento por vincular a homenet con posibles trozos que podría reutilizar de Anima, Michael Richardson presentó la familia de protocolos de Anima. El problema por resolver por parte de Anima era la unión segura de los nuevos dispositivos de red a una red empresarial. Un componente de la familia de Anima que Richardson ofreció fue «Infraestructura de inicialización de clave segura remota» (BRSKI, por sus siglas en inglés) [los otros componentes básicos de Anima —innecesarios para homenet— son «un canal seguro y dedicado (VPN) para la gestión/el control (también conocido como ACP)» y «un protocolo de señalización genérico (también conocido como GRASP)]».

Richardson dijo que un perfil de BRSKI para homenet podría ser una opción. Uno de los desafíos fue que, a diferencia de la red empresarial dirigida a Anima, las redes domésticas no son gestionadas (al menos no profesionalmente). El hecho de no poder conectarse a Wifi en primer lugar (antes de hacer la inicialización («*bootstrap*») en un dispositivo) podría causar llamadas a los proveedores o distribuidores de servicios.

Richardson también reconoció que el concepto de Anima de asignar un dispositivo candidato que comience automáticamente en una red a un cliente mediante un *voucher* que debe ser chequeado por la Manufacturer Authorized Signing Authority (MASA) podría tomarse como señal de que el IETF apoya a proveedores para que mantengan el control. Asimismo, Richardson remarcó que BRSKI era una buena conciliación entre la seguridad y la usabilidad.

DNS sobre HTTPS. Estándares listos. El WG podría cerrarse.

El DNS sobre HTTPS (DoH) acaba de comenzar, pero estima llevar su especificación a la última llamada del WG en abril de 2018, tras apenas siete meses de haberse establecido. Si no le llegan más documentos, el WG cerrará luego de finalizar con este. El DNS sobre HTTPS podría contribuir a alejar el DNS de los usuarios/desarrolladores, ya que se moldeará dentro de HTTP.

El DoH mapea cada par de consulta-respuesta del DNS en un par solicitud-respuesta del HTTP. El enfoque, según el *draft* de Paul Hoffmann (ICANN) y Patrick McManus (Mozilla), establece tipos de formateo de medios por defecto para las solicitudes y respuestas, pero «utiliza mecanismos de negociación de contenido de HTTP normales para seleccionar alternativas que puedan preferir los extremos en preparación para el abordaje de nuevos casos de uso. Además de esta negociación de tipo de medios, se alínea con las características del HTTP como el cacheo, la redirección, el *proxying*, la autenticación y la compresión».

Dos asuntos se debatieron en el grupo del WG. Uno tuvo que ver con que si debería ser igualmente obligatorio que el servidor implemente ambos mecanismos GET y POST, y hubo consenso en una respuesta positiva. Los clientes, por otro lado, serían capaces de elegir. El otro asunto en que los autores querían lograr consenso era que si debía ser obligatorio el udpwireformat. El *draft* optó por que sí lo fuera. Muchos ponentes apoyaron esta moción durante la reunión del WG, incluido Stewart Cheshire (Apple), quien observó que a medida que el DNS evoluciona, más extensiones se definirían utilizando formatos de paquetes UDP. Si pudieran ser envueltos y transportados por el UDP, sería mucho más sencillo que hacer nuevas adiciones a la respectiva extensión.

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

Hay un interés considerable y no menos importante proveniente de algunos grandes proveedores. Stephane Bortzmeyer (Afnic) presentó una visión general sobre las implementaciones (mencionadas en una lista en este sitio GitHub). Incluyen un servidor DoH operativo de Google, Akamai, y Clean Browsing. También hay varios «servidores de juguete» que implementaron el DoH. Se había logrado ya un alto grado de diversidad con cinco diferentes *software* de servidores, y cuatro de ellos con distribución pública. Las implementaciones «no eran la gran cosa», según Bortzmeyer, pero había que aclarar algunos asuntos en el *draft* en pos de aquellos que no son expertos en el DNS (por ejemplo, los de HTTP).

DNS OPORTUNISTA

Daniel Kahn Gillmore, de la Unión Americana de Libertades Civiles (ACLU), presentó lo que describió como un disparador del debate de los próximos pasos. En lugar de solo utilizar el DoH para la unión de HTTP y DNS, recomendó una suerte de mecanismo *push* (donde el servidor envía datos por sí solo) para el DoH. El servidor ubicaría en las respuestas las direcciones IP para nombres no solicitados, para que los clientes las utilicen en el futuro.

Una vez cacheados los nombres adicionales de manera local, no se necesitarían otras solicitudes de DNS. El mecanismo sería beneficioso en cuanto a privacidad y latencia. Además, para beneficiarse de la autenticación, podrían impulsarse más DNSSEC, un efecto secundario bienvenido, según Kahn Gillmore.

El «DNS *push*» no se convertirá necesariamente en un documento del WG; en cambio, debe ser acordado en los WG respectivos. El presidente del WG para HTTP, Mark Nottingham, invitó a comenzar el debate en http durante la siguiente reunión IETF.

Seguridad de la capa de Mensajería

Se comenzaron nuevos e interesantes trabajos en el BoF de Seguridad de la Capa de Mensajería. El WG que pronto será establecido quiere estandarizar una gestión de claves de grupo asincrónicos para los grupos desde dos hasta miles. Si bien el TLS permite hacer seguras las conexiones de extremo a extremo, se espera que MLS especifique un protocolo de establecimiento de clave para varios grupos de mensajería, independiente del transporte y la aplicación utilizados (incluyendo el chat, SIP, e incluso posiblemente el correo electrónico). Propuesto y presentado por autores de Cisco y Google, con coautores de Facebook (y WhatsApp), Wire, Inria y Twitter, el nivel de interés en el trabajo es altísimo.

Los elementos básicos del concepto de MLS son una autenticación (clave inicial) y un servicio de entrega (entregar mensajes, añadir o eliminar miembros del grupo) que pueden ser independientes uno del otro. La interoperabilidad de diferentes aplicaciones no es el objetivo, pero las expresiones de la potencial federación (para la autenticación) parecen variar en los documentos originales. No se establecerán nuevos protocolos de mensajería, sino que deberían reutilizarse los ya existentes (como Cose).

Las características de seguridad son el foco del nuevo protocolo. Según Richard Barnes (Cisco), no solamente incluyen el secreto hacia adelante (el contenido de comunicaciones previas protegidas tras un compromiso), sino también el secreto poscompromiso —PCS, por sus siglas

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

en inglés. (El contenido de la comunicación estará protegido luego de cierto punto, tras ocurrido un compromiso). La gestión de claves estandarizada y segura para las comunicaciones de grupo fue, por un tiempo, el desiderátum, según señaló un ingeniero de Matrix.com.

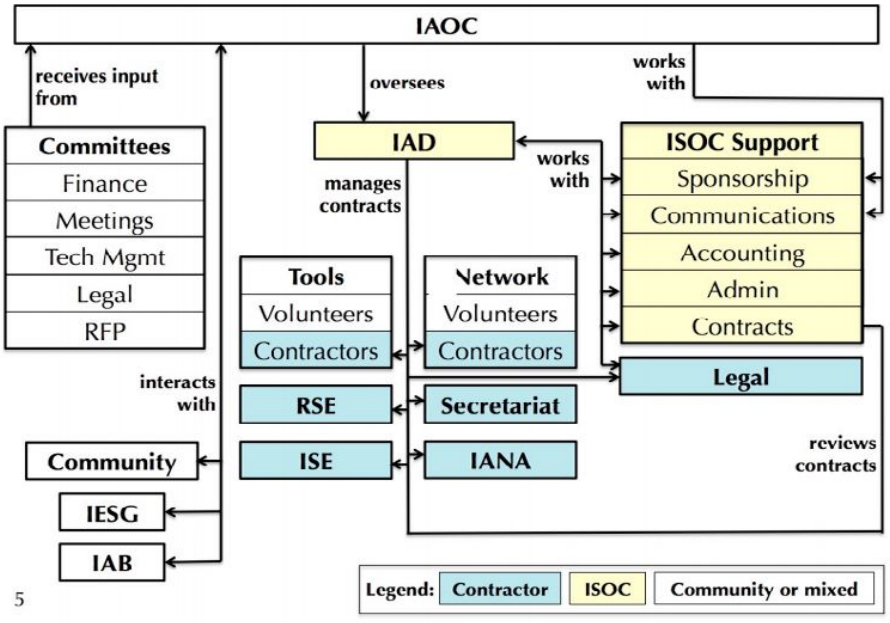
El BoF ya opinó sobre un punto de la carta constitutiva para el trabajo que señala que una extensión de «visibilidad» (lo que implica que el protocolo incluiría la capacidad de descifrado para terceros fuera del grupo) queda excluida. La formulación de este punto cambió en el debate y algunos pidieron no abordar el asunto en lo absoluto.

Puede encontrar el documento de la arquitectura aquí, y las especificaciones base aquí. Puede echarle un vistazo al cifrado detrás del concepto en este documento académico sobre «Asynchronous Ratcheting Tree».

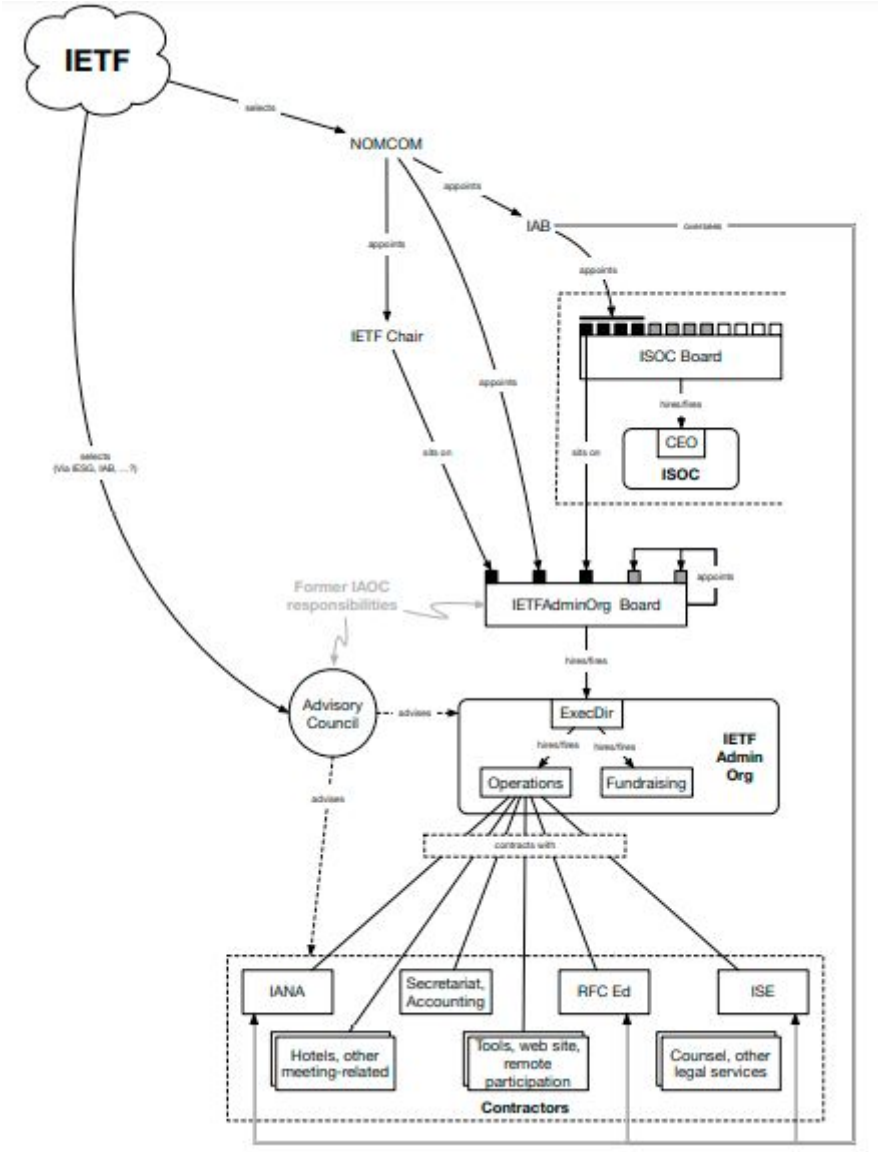
IASA 2.0

Por algún tiempo, la comunidad del IETF ha intentado decidirse sobre la futura relación con la Internet Society (ISOC). Durante su reunión en Londres, el BoF de IASA 2.0 decidió seguir adelante y establecer una Sociedad de Responsabilidad Limitada (LLC) para las operaciones administrativas del IETF. Como filial, la ISOC.org tomará control de su financiación y contratación. El IAOC, comité administrativo del IETF, puede ser reemplazado por una Junta Directiva (vea el *draft* de Brian Habermann et al.).

Los integrantes de la Junta, la interface a la comunidad (¿Consejo Asesor?) y otros detalles (incluido el posible final de la Fundación del IETF y mantener los DPI de la serie de RFC con la LLC) son cuestiones que habrá que debatir en un futuro Grupo de Trabajo. Vea el gráfico de posibles detalles con respecto a los nuevos organismos y el gráfico más abajo, que da una visión general del asunto:



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



La decisión con respecto al modelo de filiales (en lugar de mantener el statu quo o cortar los lazos con ISOC por completo) debe recibir confirmación en la lista de correos, según anunció la presidente del IETF, Alissa Cooper, durante la reunión Plenaria. Un WG resolverá los detalles y actualizará el viejo BCP 101 y la IASA.

Los textos jurídicos para la LLC se redactarán por fuera del WG, tarea que realizarán los abogados (durante la reunión plenaria, el IETF presentó sus dos nuevos abogados: Brad Biddle, Biddle Law PC, David Wilson, Thomson Hine LLP).

Aunque hubo consenso en el modelo de LLC, no todos votaron a favor de la nueva estructura de IASA. Avri Doria, presidente del Grupo de Investigación sobre las Consideraciones de los

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

Derechos Humanos en los Protocolos (HPRC) le dijo a quien escribe que estaba preocupada por la responsabilidad del organismo de estandarización.

PROBLEMAS PRESUPUESTARIOS SIN RESOLVER

En uno de sus aspectos, la reforma organizacional no cambiará mucho. Aunque el IETF podrá contratar y no asumirá a la ISOC como un techo legal, seguirá llegando desde la ISOC una buena cantidad de dinero para utilizar.

Andrew Sullivan, el nuevo presidente del IAOC, presentó el presupuesto y explicó la brecha financiera a la que se enfrenta el organismo de estandarización una vez más en 2018. Si bien los gastos son estables y el presupuesto para 2018 es casi el mismo que el de 2017 ($7M), la asistencia a las reuniones viene decreciendo. Por lo tanto, para el 2018 el IAOC calculó que habrá una brecha de $ 300.000 de asistencia paga. El monto será cubierto una vez más por ISOC, pero el IAOC, en un intento de hacer que el IETF dependa menos de la ISOC financieramente, aumentará las tarifas de las reuniones (más del 10 por ciento en 2019 de actualmente $ 700, comenzando en 2020 por un tres por ciento anual).

Hubo discusiones sobre el aumento de las tarifas de las reuniones, en las que dos participantes de países africanos (los dos *fellows* de ISOC) advirtieron sobre el incumplimiento del objetivo de hacer que el IETF sea más global e inclusivo.

Los efectos de IASA 2.0 en la situación financiera no están claros, según Sullivan.

Se contrató un nuevo recaudador de fondos de patrocinios (Ken Boyden) para que siga entrando dinero de patrocinadores.

IASA 2017 Actuals, 2018 Budget & 2019-2020 Advice				
	2017	2018	2019	2020
Meeting Revenue	$4,205,690	$3,908,825	$4,153,950	$4,419,028
ISOC Direct Contribution	$2,647,378	$3,007,774	$2,932,599	$2,702,260
In-Kind Contribution		$113,000	$113,000	$113,000
Total Revenue	$6,853,068	$7,029,599	$7,199,549	$7,234,288
Total Meeting Expenses	$2,994,744	$3,089,369	$3,170,545	$3,213,560
Total Operating Expenses	$3,858,323	$3,940,230	$4,029,004	$4,020,728
Total In-Kind Contribution		$113,000	$113,000	$113,000
Total Expenses	$6,853,067	$7,029,599	$7,199,549	$7,234,288
ISOC Direct Contribution w/Cap Invest	$2,713,004	$3,320,771	$3,145,552	$2,925,294

IANA.com fue transferido de ICANN a la Fundación de IETF el 8 de marzo. Se completó la transferencia de IANA.org y de IANA.net la semana previa a Pascuas.

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

IEPG sobre DNS: algunas recomendaciones

El Grupo de Ingeniería y Planeación de Internet, establecido para crear una interface entre operadores e ingenieros de protocolos y que se reúne regularmente antes de la reunión del IETF, tenía un gran número de presentaciones sobre el DNS en su agenda.

Giovane Moura (SIDN Labs) presentó cinco recomendaciones para los operadores de DNS que emanan de los resultados de trabajos académicos. Las recomendaciones son las siguientes:

R1: Todos los autoritativos deberían tener una latencia similar.

R2: El ruteo puede ser más importante que las ubicaciones

R3: Los mapeos anycast detallados requieren mediciones activas

R4: Bajo estrés, dos estrategias

R5: La infraestructura compartida corre el riesgo de daño colateral durante ataques

Mitigación de respuestas truncadas

Una propuesta de Geoff Huston y Joao Damas apunta a mitigar los problemas con las respuestas truncadas. El DNS sobre UDP no funciona en el IPv6 y la fragmentación está muy poco soportada. El concepto de ATR es enviar un paquete con una bandera TR (truncada) detrás del paquete truncado. Si el cliente recibe la respuesta fragmentada, se ignorará el paquete ATR. Si la respuesta fragmentada no llega al cliente, el ATR probablemente sí lo hará, y el cliente se trasladará al TCP.

Remoción de los métodos para esquivar problemas de EDNS

ISC (Bind), .CZ (knot), NLnetlabs (unbound), y PowerDNS eliminarán los métodos para esquivar problemas en las implementaciones EDNS0 rotas, y solo permitirá respuestas estándares a partir del 01/02/2019. Para pruebas, diríjase a:

https://ednscomp.isc.org/ednscomp/

El conjunto de pruebas de código abierto:

https://gitlab.isc.org/iscprojects/DNS-Compliance-Testing

Registros DS paralizados

Si hay un registro DS sha-256, los resolutores no utilizarán los registros DS con sha-1. Luego de que varios TLDs se firmaran incorrectamente porque se introdujo un registro DS para una DNSKEY no existente, ICANN ahora busca mitigar el hecho de que, actualmente, no existe una fórmula de prevención del modo de fallo donde se ignora el DS con SHA1 en presencia de SHA2.

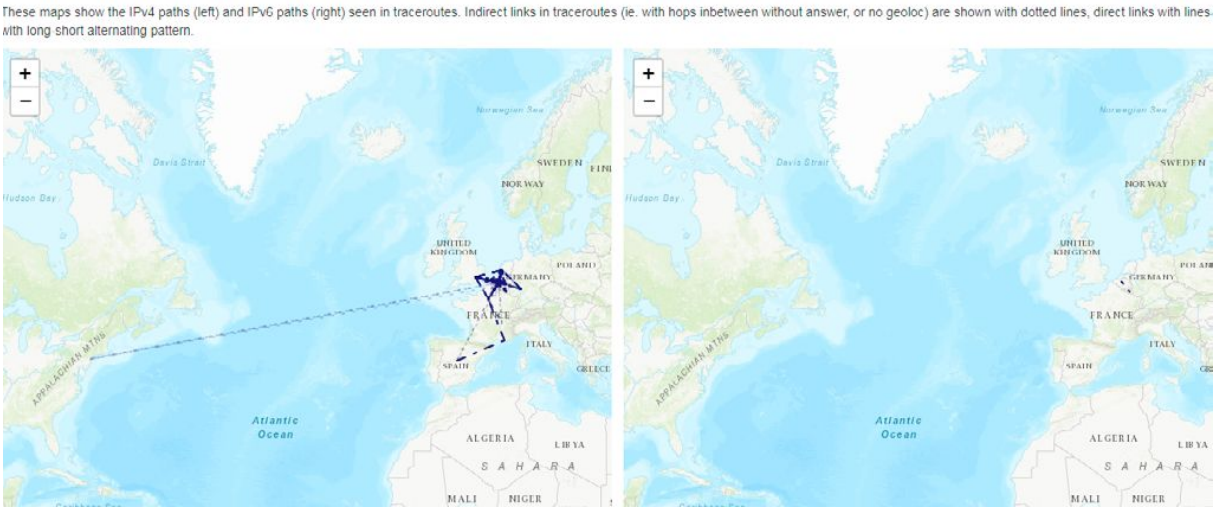
Roy Anders presentó las recomendaciones de ICANN:

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

- Ser coherentes en el uso de tipos de «digests» en registros DS.
- Usar el mismo tipo —o tipos— de «digest» para todas las KSK.
- No recurras a tus mayores para que lo resuelvan por ti.
- Estamos en 2018. No es necesario usar SHA1, se puede usar de manera segura SHA256.
- No rotar la KSK y el tipo de «digest» DS al mismo tiempo. Elegir uno o el otro.
- Si existen «Mejores Prácticas Vigentes» (BCP) 3 de las DNSSEC, deberían incorporarse.
- Hay 8 dominios de nivel superior que solamente usan SHA1. Todos los demás son SHA2 o duales, SHA1 y SHA2.

Más contenido interesante del IEPG

Dos mediciones son interesantes: una es el [proyecto RIPE IXP Country Jedi](), que permite mostrar cómo ocurre la conectividad de usuario a usuario dentro de un país:



La otra tiene que ver con los resolutores del DNS públicos: ¿qué [servidores raíz usan los resolutores]()? La medición de ICANN demuestra que hay 20 por ciento de «respuestas extrañas».

De las 25.881 direcciones analizadas:

- 16.835 devolvieron una respuesta (65%)
- 13.826 devolvieron el registro SOA esperado

  De esos registros SOA:

  - 13.800 devolvieron números de serie SOA esperados (como máximo 2 días de desfase)
  - 5 tenían un número de serie SOA con diferente formato (1520976703)
  - 21 tenían un número de serie desactualizado (el más antiguo es 2012041813)
  - 3.009 devolvieron un registro SOA inesperado (mname completamente diferente, etc.)

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

- De aquellas que respondieron, el 22% (3009 de 13.826) tienen otros servidores raíz configurados.

La próxima reunión del IETF tendrá lugar en Montreal, del 14 al 20 de julio de 2018.

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