Informe de CENTR
IETF98

Chicago, 26-31 de Marzo 2017

Traducción - LACTLD

LACTLD agradece a Hugo Salgado (nic.cl), por la revisión de la Edición en Español

Para acceder a la versión en inglés de este informe ir a Highlights de: **https://centr.org/**

Aspectos destacados

IASA 2.0: ¿Debe el IETF reinventar su estructura organizacional?

10 años después de que el IETF rompiera lazos con su antiguo organismo secretarial CNRI y que haya asumido las responsabilidades de las funciones administrativas, la organización ha crecido más que la sociedad de apoyo administrativo (IASA) del IETF. En este caso, "crecido" no significa que la organización ha aumentado su tamaño: es más bien que el conjunto de tareas ejecutadas por la estructura administrativa se ha vuelto más voluminosa e incluso por momentos más difícil, como por ejemplo los problemas con las visas e ingresos a EEUU. En una reunión BoF ("birds of a feather", acrónimo que representa una reunión de discusión informal) sobre el posible futuro de la IASA, se le preguntó a la comunidad si ajustes menores a las estructuras actuales de IASA y IAD serían suficientes, o si era necesaria una mayor revisión del sistema, incluyendo un cambio radical de la naturaleza jurídica de la IETF.
Dos cuestiones importantes se ciernen en torno al proceso de un nuevo paso hacia la reforma del cuerpo de estandarización, iniciado por el actual presidente del IETF, Jari Arkko: (1) Cómo reorganizar el IETF para avanzar hacia la toma de control organizacional y trazar una línea clara entre sí mismo e Internet Society (ISOC), patrocinador principal y actual hogar legal del IETF; y (2) cómo asegurar un financiamiento estable a futuro.

¿Recuperar el control de ISOC?

Actualmente, el IETF permanece como un foro de estandarización no incorporado. Por lo tanto, ISOC proporciona el estatus legal necesario para la contratación de personal, hoteles, reuniones, patrocinadores y otros proveedores de servicios.
La presidente de ISOC, Kathy Brown, señaló en la sesión Bof de la IASA que el IETF "quiere ser independiente, pero se encuentra dentro de una organización que debe de tomar decisiones dependientes de su estatus legal". Brown aseguró a los participantes que ISOC está dispuesta a asociarse con el IETF en el doble esfuerzo de posibles reformas estructurales y financieras. Aun así, sigue mostrándose como una inquietud dicha relación entre los participantes del IETF. Se han formulado preguntas sobre cuánto del personal de ISOC estuvo involucrado en lo que hizo IAD, dijo la presidente entrante de IETF, Alissa Cooper, en su esbozo para las discusiones.
La creciente lista de tareas llevadas a cabo por ISOC para la IETF cae en dos categorías: La primera es la ayuda más fútil que es la sostenibilidad financiera de la IETF (con una contribución anual de aproximadamente 2,3 millones de dólares y apoyo a las insuficiencias de las reuniones como los eventos costosos, pero menos concurridos como el de Buenos Aires). El personal de ISOC también brinda soporte al alcance de los patrocinadores y ha contribuido con dinero para el fondo.
La segunda categoría de tareas es la parte más efímera del desarrollo de una comunidad tan diversa para la IETF, tanto geográficamente como en relación con los grupos de partes interesadas. ISOC financia y organiza programas de becas para ingenieros de países en desarrollo y de reguladores. ISOC también patrocina varias actividades académicas: Premio de trabajo a la investigación de red aplicada (Applied Network Research Paper Award), Talleres de investigación de red ACM ISOC (ACM ISOC Networking ResearchWorkshops) , Taller de seguridad de redes y sistemas distribuidos (Network and Distributed System Security Workshop), y la más reciente

edición de la Privacidad Online y DNS, y las publicaciones en el seminario de IETF.
Considerando el gran número de programas, como también el hecho de que el personal de ISOC está involucrado en varias tareas administrativas y prácticas el IETF; ambas organizaciones parecen pegadas entre sí. Varios problemas que derivan de esta situación se mencionaron durante el BOF de la IASA. Varios patrocinadores grandes como Cisco, Comcast y Ericsson realizaron declaraciones bastante similares, sobre el problema de explicar por qué el financiamiento ofrecido fue a ISOC cuando en realidad el patrocinio era para la IETF. Otro tema presentado por Alissa Cooper fue que el IETF no tiene "un montón de supervisión sobre la contratación y el rendimiento" del personal asignado por ISOC para realizar las distintas tareas para la IETF.
Incluso hubo alguna animosidad expresada contra ISOC. Randy Bush de IIG pidió a el IETF que recuperara “cosas” como el programa de difusión y dijo que "sin el IETF, ISOC no duraría más de tres años". Parece emerger una ligera tensión de esa declaración sobre quién debe estar en el asiento de conducción: ISOC, quién a través de los registros PIR y .org tiene ahora un margen de maniobra financiera considerable y ha crecido a cerca de 100 funcionarios, o la no-organización IETF, que ayudaron a crear la ICANN (y, por ende, el mercado de los dominios).

¿Operación quirúrgica o borrón y cuenta nueva?

Una gran pregunta que plantearon varios participantes en Chicago fue si la IASA 2.0 debería ser una mejora de la estructura actual o si se necesita una reforma más radical. A partir de estas discusiones, uno puede sacar la conclusión de que existe una tendencia hacia una solución más sustancial. Tanto el entrante como el saliente presidente de IAB advirtieron que solo trabajarían para "tapar agujeros".
Andrew Sullivan de Oracle-Dyn dijo que encontró que "la estructura (es) demasiado débil por lo que necesita cambios significativos". La sobrecarga de tareas administrativas en algunas posiciones, como por ejemplo en la presidencia de la IAB – ha demostrado ser un error. Hardie, el nuevo presidente de la IAB se quejó que la IAB había perdido a uno de los expertos más finos en DNS e internacionalización en Andrew Sullivan, puesto que durante la tenencia IAB de Sullivan, había sido abrumado con tareas, además del gran número tareas ex officio del presidente del IAB . Tratar de solucionar este problema estructural mediante simplemente invertir más recursos no ayudaría, y sería similar a "más gente pasando datos por la API incorrecta".
La conclusión de Cooper sobre esta temática fue que existe "una apertura a realizar cambios considerables" con respecto a la estructura organizacional. Ella dijo que prepararía un documento inicial para la discusión. Más BoFs y Webinars (como el que está en proceso de elaboración para el Bof de la IASA) se celebrarán en los próximos meses.

Preocupaciones sobre el impacto de pasar de voluntarios a profesionales

Otro motivo de preocupación mencionada por miembros asiduos del IETF -incluyendo a Lucy Lync, Bob Hinden y Randy Bush- fue que el IETF podría redireccionarse de una base de voluntariado y un cuerpo autónomo, a un cuerpo profesionalmente dirigido. Un incremento en el personal profesional podría resultar en que el personal tuviera una influencia mayor sobre cómo evoluciona el IETF. "Esto va en contra el espíritu de la IETF", dijo Lynch. Se apuntó hacia el W3C.
Cooper y otros tantos objetaron que existe una conexión directa entre el personal más profesional y la pérdida del carácter autónomo de gobierno. Olaf Kolkman (quién había presentado los números finales sobre los trabajos llevados a cabo por ISOC para el IETF) dijo que, debido al cambio en la industria, el grupo de voluntarios fue disminuyendo. Esto hace difícil depender

solamente de voluntarios para llevar a cabo todas las tareas necesarias que permiten tener una buena experiencia IETF para desarrolladores. Cooper ciertamente favorece un enfoque pragmático.

Situación financiera: no es extrema (todavía), pero requiere tomar acciones

Se le encomendó a Arkko investigar la situación financiera. En Chicago, él dijo que la situación financiera no era "grave, pero tenemos que hacer algo al respecto". También dijo que el gran problema con respecto a la asistencia paga es que se ha mantenido estable, mientras que los costos van en aumento. Sin cuotas de asistencia más altas, los costos e ingresos de las reuniones no se cotejan ni coinciden. Mientras que ISOC intervino en Buenos Aires, la disminución de la asistencia de las reuniones con sede en Estados Unidos se evaluó a través de un cuestionario especial sobre las potenciales preocupaciones de los asistentes sobre cuestiones de las políticas de visado de Estados Unidos.

Cambio de presidencia

En Chicago, Alissa Cooper (Cisco) asumió el puesto de Jari Arkko (Ericsson) como presidente del IETF. Cooper será la primera mujer presidente del IETF. Aunque la diversidad de género claramente ha mejorado entre los organismos homólogos del IETF, varios observaron que hay tres empleados de Cisco en el equipo directivo (IESG): Alissa Cooper, Benoit Claise y Álvaro Retana. A modo de comparación, el competidor directo de Cisco, Juniper, tiene solo un lugar en la banca, mientras que el fabricante chino Huawei, así como otros posibles jugadores asiáticos, se encuentran curiosamente ausentes.

Dado que los Estados Unidos se encuentra una vez más en duda como un espacio de encuentro, el hecho de que todas las posiciones de la presidencia del IETF, IAB y IRTF se encuentran ocupadas por ciudadanos estadounidenses puede parecer un hecho poco afortunado.

Los debates sobre las cuestiones de visado parecen continuar, ya que los números de cuotas de asistencia pagadas para la reunión de IETF en Chicago se redujeron (sólo unas pocas docenas más que la reunión en Buenos Aires). Está circulando una encuesta para entender las cuestiones de visa que podrían representar un problema constante. Está previsto que el IETF101 se celebre en San Francisco (para más información sobre estas discusiones ver la sección "lugar de reunión GT" más adelante).

El presidente Jari Arkko se marchó entre una ovación de aplausos durante su fiesta de despedida, y fue retratado como un trabajador incansable por Alissa Cooper, su sucesora. Arkko fue electo en la transición de IANA y las secuelas de la caída de Snowden, y tuvo que lidiar con cuestiones políticas más allá de lo esperado. Arkko continúa en el papel de miembro de la IAB.

¿Los derechos humanos deberían ser parte de la "lucha"?

El debate sobre la estandarización de los derechos humanos ha subido de categoría: la reunión del IETF en Chicago vio una discusión en el plenario sobre la ética de la elaboración de estándares y responsabilidades para los ingenieros.

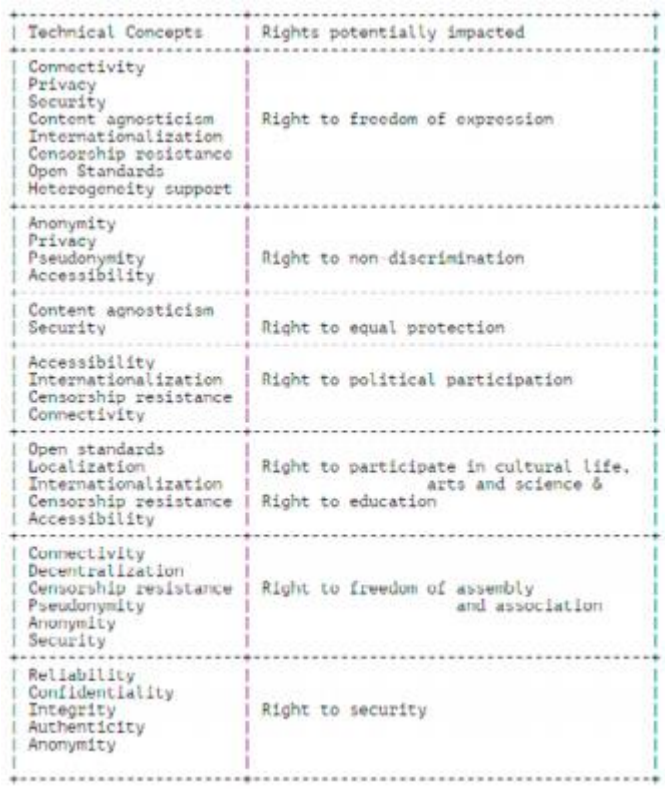
Así, haciendo que los conflictos de intereses sean parte de la lucha y tratar de inclinar el campo de acción.

Dave Clark, autor del famoso libro "Tussle in Cyberspace", (lucha en el ciberespacio) dijo que la pregunta más importante para los ingenieros era si eran lo suficientemente inteligentes como para inclinar el campo de juego al formar el diseño de sus propios estándares (la presentación en el

plenario de Clark puede ser consultada aquí). Contemplando el "debate Raven", Clark destacó que había resultado que era una de las decisiones más eficientemente documentada y divulgada por la IETF de carácter político: rechazar la estandarización de las intercepciones de la ley CALEA. En retrospectiva, Clark acotó, los ingenieros renunciaron a "inclinar el campo de juego" al no incrustar en la lucha – ni los intereses conflictivos de los diferentes actores – directamente en la norma. Al negarse a integrar los intereses de aplicación de la ley y, en cierto modo, moldeando cómo la intervención de teléfonos sería dentro de la norma, desviaron la aplicación de la ley a diferentes actores con ningún interés potencial en inclinar el campo de juego.
Otro ejemplo interesante se mencionó durante el debate de Mike Bishop, ingeniero de Microsoft y uno de los autores de Quic protocol suite. Bishop señaló que hubo trabajo adquirido al organismo de standares de IEEE sobre multiContext TLS, "un protocolo de comunicaciones seguro que extiende TSL para permitir la incorporación de middleboxes en las sesiones seguras". De forma más simple, es una forma de romper la TLS. No hablar de la lucha de la encriptación a través de los intereses de los administradores de red o la aplicación de la ley y el hecho de conducir estos intereses lejos de la IETF, resultó en que dichas soluciones se prepararan en cualquier otro lugar sin siquiera pedir al cuerpo de estandarización de TLS para comentar los posibles efectos finales.
Así, mientras Clark claramente reconocía la necesidad de hablar de los derechos humanos en el diseño de la tecnología, en integrar científicos sociales, abogados y técnicos, expresó su apoyo al movimiento del "value based design movement", y abogó para incluir intereses divergentes tanto como sea posible en el propio diseño.

Consideraciones de los derechos humanos en los protocolos en la IRTF

La IRTF inció este camino en el Grupo de Investigación de Consideraciones de Derechos Humanos en Protocolos. Niels ten Oever, el co-presidente del RG, presentó un resumen de su trabajo. La RG HPRC ha finalizado su extenso documento sobre " Research into Human Rights Protocol Considerations" ("Investigación sobre las consideraciones relativas al Protocolo de Derechos Humanos") que intenta corresponder conceptos técnicos y derechos humanos (ver lista a continuación) y que actúe como pauta para los diseñadores. Ten Oever pidió a los ingenieros que consideraran la posibilidad de adoptar consideraciones sobre derechos humanos en la IETF estableciendo un grupo de trabajo sobre derechos humanos.



Technical Concepts	Rights potentially impacted
Connectivity Privacy Security Content agnosticism Internationalization Censorship resistance Open Standards Heterogeneity support	Right to freedom of expression
Anonymity Privacy Pseudonymity Accessibility	Right to non discrimination
Content agnosticism Security	Right to equal protection
Accessibility Internationalization Censorship resistance Connectivity	Right to political participation
Open standards Localization Internationalization Censorship resistance Accessibility	Right to participate in cultural life, arts and science & Right to education
Connectivity Decentralization Censorship resistance Pseudonymity Anonymity Security	Right to freedom of assembly and association
Reliability Confidentiality Integrity Authenticity Anonymity	Right to security

La petición del IETF sobre los derechos humanos generó reacciones adversas. Una fracción más pequeña sostuvo que el IETF podría no ser el organismo correcto dada la falta de experiencia en el campo (Paul Hofmann, ICANN, Pete Resnick, Qualcom) También se cuestionó sobre cómo el HPRC RFC sería implementado (por ejemplo, Mirja Kühlewind, ETH Zurich). No es clara la correspondencia entre los derechos y conceptos técnicos.

Esto se hizo evidente en la primera discusión sobre el nuevo trabajo propuesto por ten Oven para el HPRC. Como analogía al existente documento "Privacy Considerations" (Consideraciones acerca de la privacidad), ten Oever presentó "algo que quedó claro en las discusiones iniciales sobre el nuevo trabajo de HPRC sobre *anonimato* y *libertad de asociación*". La negación distribuida de servicios, que algunos activistas defendieron como una forma potencial de protesta hace años, no está en línea con la libertad de asociación, abogó ten Oever, debido a la interrupción del tráfico legítimo, como ejemplo.

Pero a pesar de la reticencia de los participantes del IETF a involucrarse en una discusión de HPRC, la mayoría expresó su entendimiento a que los diseñadores no pueden escapar a los posibles efectos sociales de las decisiones del diseño. "Inclinaremos el campo de juego", dijo el ex presidente de IETF Harald Alvestrand. Los ingenieros sólo pueden tratar de inclinarse en una manera consciente, sin la garantía de tener éxito. Daniel Kahn-Gilmor de la Unión Americana de libertades civiles, subrayó que sin lugar a dudas, hay ingenieros que tuvieron que abordar la ética en su trabajo.

Consideraciones éticas sobre el trabajo de estándares están muy de moda últimamente, con el IEEE ejecutando una iniciativa (véase WG y BoFs, HPRC a continuación) y esfuerzos similares en la ISO.

El nuevo transporte de protocolo Quic avanza rápidamente

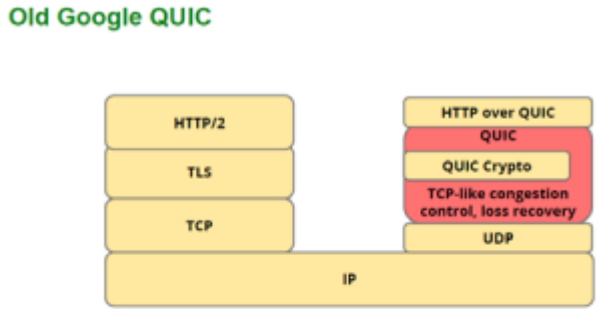
La estandarización rápida es posible, como lo demuestra Quic. El nuevo protocolo de transporte UDP desarrollado por ingenieros de Google, que se mantuvo lejos de estandarización del IETF en el año 2014, será empujado hacia el primer borrador de la implementación de RFC dentro de un año, tal como lo confirmó Lars Eggert, co-presidente del Quic Working Group ("grupo de trabajo Quic").

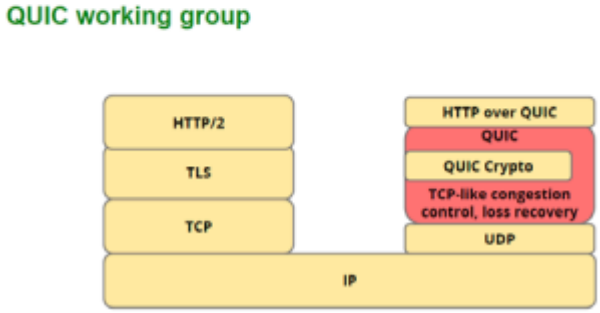
El grupo de trabajo fue avanzando a un "ritmo vertiginoso," dijo el ingeniero de Google y autor del documento Jana Iyengar. El grupo de trabajo ya tuvo una reunión entre períodos de sesiones en Tokio en enero; se reunirán de nuevo en París en junio antes del IETF99 en Praga y hay planes para un tercer encuentro antes del IETF100. Es en estas reuniones entre períodos de sesiones (con 50 participantes en Tokio) donde se logra un gran progreso, según los observadores.

Quic no será sólo Quic de Google, Iyengar ha subrayado en un Tutorial Quic del domingo antes de la reunión de Chicago. Los cambios incluyen el formato de la cabecera y la sustitución de encriptación propietaria de Google con TLS 1.3, la cual ha tratado de mantener el ritmo de Quic para estar listo para el nuevo protocolo de transporte.

Los comentarios del presidente de la IETF Jari Arkko ilustran perfectamente el posible impacto de Quic. Arkko dijo a este reportero que el desarrollo de Quic fue una de las sorpresas en su mandato. Él había pensado que un alejamiento del modelo TCP no era posible. Eggert dijo que espera que Quic se encargue rápidamente de hasta el 60-70 por ciento del tráfico de la web. Dado que los grandes navegadores y proveedores de software insisten en Quic (Google, Mozilla, Microsoft), el cambio sucedería aún más rápido, Eggert dijo a esta reportera.

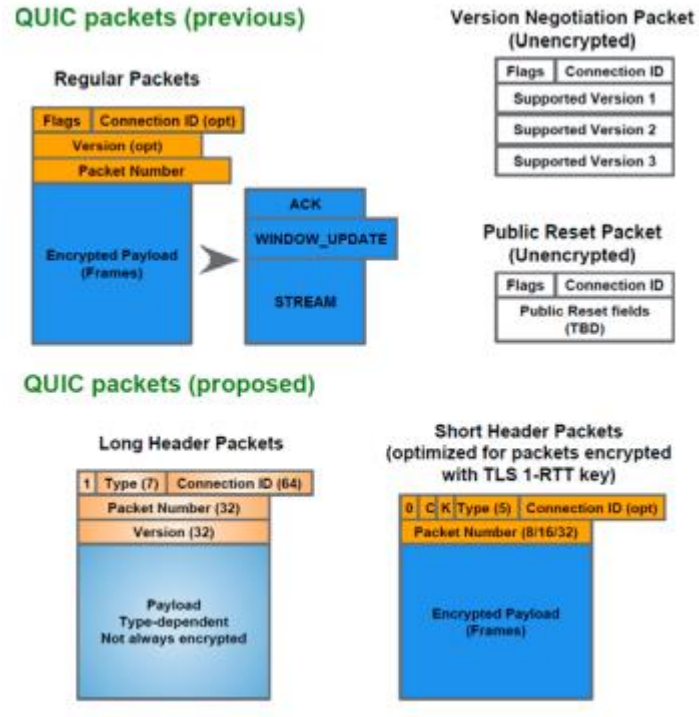
Se ha expresado el interés de trabajar en otros paquetes HTTP sobre Quic, por ejemplo, DNS sobre Quic. Será muy interesante observar cómo el éxito de Quic afectará el desenvolvimiento de una TCP más segura, en TCPinc, pero también, si DNS sobre Quic es estandarizado, DNS sobre TLS. Podría haber trabajo para los defensores de la privacidad en la evaluación de cómo Quic comparó las versiones TLS seguras de tráfico.





Formato de cabecera resuelto

Llegar a un acuerdo sobre el formato de encabezado Quic fue un gran problema que fue resuelto antes del IETF en Chicago para luego ser presentado allí mismo.



La nueva cabecera de Quic IETF tiene dos versiones: una cabecera larga (iniciando con bit en 1 que indica que efectivamente es la cabecera larga), un campo tipo de 7 bit, una ID de conexión de 64 bit y un paquete con la versión y el número de aviso (cada uno de 32 bit), además de la sección de

datos (payload). La cabecera larga se utiliza para establecer la primera conexión entre servidor y cliente. El saludo (handshake) no está encriptado, pero sí autenticado. Luego del saludo, y para conexiones con un servidor conocido, la cabecera reducida puede ser utilizada, la cual solo necesita un campo de tipo 5 bits, y hasta 32 de número de paquete. El identificador de conexión sigue siendo una opción. El payload está totalmente encriptado.

En el Quic original, la versión tuvo que ser testeada; ahora, la información de la versión se encuentra en la cabecera, y aunque la visibilidad se ve levemente disminuida, fue un cambio aceptado por los autores. El Quic del IETF es ahora "más limpio", dijo Iyengar.

Iyengar subrayó que el nuevo protocolo reutiliza un número de ideas existentes, como el TCP Fast Open (T/TCP) y la labor actual de TLS 1.3, incluyendo un establecimiento de conexión más rápida. El establecimiento de la conexión 0RTT fue una contribución significativa al Quic. Para permitir las conexiones 0RTT, TLS 1.3 introduce el envío de parámetros de DiffieHelman y especialmente las extensiones de claves públicas *KeyShare*. Se trata de nuevas extensiones que se encuentran dentro de los mensajes de ServerHello y ClientHello Otra idea reutilizada es utilizar corrientes multiplexed sobre una conexión (también usado en el protocolo basado en TCP y desarrollado por Google llamado Speedy).

Varios proveedores de Middlebox y operadores de red no están contentos con el tráfico encriptado.

Al reducir la información en la cabecera, Quic reduce la visibilidad y las opciones de rastreo de "meta data". Mientras que la información TCP podría quitarse del campo de cabecera, Quic no es tan práctico como para lograrlo. La discusión acerca de visibilizar bits adicionales para la gestión de red y resolución de problemas podría ser la más difícil de todas, piensa Iyengar.

Una propuesta de Mirja Kühlewind, Director del Área de Transporte (ETH Zurich), es que un número de números de paquetes haga eco para permitir el monitoreo pasivo de middleboxes. Kühlewind preguntó si alguien objetaba, y algunos participantes advirtieron que debería estar permitido dar un paso atrás con respecto a un posible desenfoque de la información de conexión. Potenciales problemas con la privacidad podrían entenderse en un futuro, dijo Daniel Kahn Gilmor de ACLU.

Uno de los editores de Quic dijo que hubo charlas intensivas con los proveedores de middlebox, pero si fuera el caso que los operadores de red y los vendedores de middlebox no daban pruebas amplias sobre el problema que tenían, no había mucho incentivo para que el WG permitiera los bits adicionales. En línea con la pregunta sobre la lucha (véase arriba), el GT (grupo de trabajo) tendrá que llegar a una decisión si rechazan las solicitudes de los operadores y permanecen más en el lado de la privacidad. Parece un claro caso de prueba para el HRPC.

home.arpa en vez de . . . ¿.HomeNet?

En Chicago, todavía estaban en desacuerdo sobre qué TLD debe ser utilizado para el direccionamiento en el HomeNet. Esta situación cambió con la publicación de una enérgica declaración por parte de IAB sobre la diferencia entre la reserva especial de dominio (non-DNS use) y nombres especiales destinadas explícitamente a trabajar con el DNS (que se declaró que necesita estar bajo un .arpa u otro TLD administrado por IAB) Una semana después de la reunión del IETF, una nueva versión del proyecto homenet se publicó pidiendo home.arpa.

En las dos semanas anteriores al evento de Chicago, participantes de IETF y los representantes ICANN (más que nada el Presidente del Consejo de ICANN, Steve Crocker) se habían enfrentado en

la lista de correo de HomeNet sobre el proyecto de propuesta sobre .HomeNet, de que no sólo estuviera reservado como un TLD de uso especial, sino también delegado en la zona de la raíz. Otro punto de la contención fue también que los autores no quieren tener el nuevo TLD firmado con DNSSEC, ya que tenerlo firmado puede resultar en una falla de validación debido al uso local. Con DNSSEC, un resolutor "stub" de validación rechazaría la resolución de nombres publicados en el servidor de nombres .home.arpa.

En este momento lo que todavía no está claro es cuanta visibilidad externa para los nombre hogareños desean los autores de la arquitectura homenet.

Hablando con esta reportera, Ted Lemon, uno de los fundadores de Nominum y principal proponente del proyecto, argumentó que su comprensión del MOU de ICANN de la IETF claramente permitía a la IETF iniciar esas delegaciones. Lemon aludió en particular a la sección 4.3 del Memorandum de Entendimiento (aprobado en el año 2000) que lee

Nótese que (a) las asignaciones de nombres de dominio para usos técnicos (como nombres de dominio para buscar DNS inversa), (b) las asignaciones de bloques de direcciones especializados (como los bloques multicast o Anycast) y (c) las asignaciones experimentales no se consideran políticas y quedará sujeto a las disposiciones de la presente sección 4. (Para efectos de este memorandum, el término "asignaciones" incluye las asignaciones). En caso de que ICANN adopte una política que le impida cumplir con las disposiciones establecidas en la sección 4 con respecto a las tareas descritas en (a) - (c) arriba, ICANN notificará al IETF, que entonces puede ejercer su capacidad para cancelar este Memorandum según la sección 2 anterior".

De acuerdo con la propuesta de Lemon el IETF debe iniciar tratativas con ICANN sobre la asignación de .homenet – y utilizarlo como una oportunidad para aclarar los desacuerdos sobre la interpretación.

La petición de Lemon se encontró con una resistencia considerable en la reunión homenet de Chicago. El Director de Área, Terry Manderson, recordó al grupo de trabajo que la petición de una introducción insegura en la zona de la raíz no fue "cubierta en términos de la política IETF" y "un nuevo proceso tendría que ser construido con ICANN". El director Jari Arkko recordó al grupo de trabajo "ser realmente claro en cuáles son las implicaciones de ciertos requerimientos", agregando que el proceso podría ser más largo. El presidente en vías de retirarse Andrew Sullivan de IAB (Oracle/Dyn) también advirtió que abrir el memorando de entendimiento con ICANN podría incluso ser desventajoso para el IETF.

Hubo considerable crítica con respecto a la tratativa DNSOP con respecto a la problemática de los nombres especiales. Al final, estas advertencias resultaron en que Lemon y su co- autor Pierre Pfister (Cisco) cambiaran su propuesta y fueran para home.arpa. Sin embargo, Lemon incluyó una leve diatriba sobre un tema que tiene con home.arpa:

"Algunas interfaces de usuario de descubrimiento de servicio que se espera se utilicen en homenets ocultan información como nombres de dominio de los usuarios finales. Sin embargo, todavía se espera que en algunos casos, los usuarios tendrán que ver, recordar e incluso escribir, nombres que terminen con '. home.arpa'. Por lo tanto, es deseable que los usuarios identifiquen el dominio de primer nivel y entiendan que al utilizarlo expresa la intención de conectarse a un servicio específico para la red doméstica a la que están conectados. Imponer el cumplimiento de este propósito está fuera del alcance de este documento."

Características eliminadas del borrador de arquitectura

Un suavizado nuevo borrador sobre la nomenclatura de arquitectura no incluye visibilidad externa y desiste de otras propiedades planificadas en versiones anteriores del documento. La nueva nomenclatura de arquitectura no tiene un modelo de seguridad, ninguna noción de "estado", ninguna manera limpia de enumerar todos los servicios, y ningún lugar para recoger la enumeración de los servicios (mDNS fue, dijo Lemon durante el GT, un "Protocolo defectuoso" en ese sentido). mDNS, dijo Lemon, no estaba proporcionando un identificador único por dispositivo. Usar una heurística para posibles problemas de conflicto de nombre está en discusión, pero permitiría algunos casos limítes.

Lemon dijo que optó por la nueva nomenclatura arquitectura de documento reducida para conseguir que avance. La duda para un protocolo de registro se podría solucionar más adelante en DNSSD, él dijo. También dijo que el grupo de trabajo todavía podría hacer un segundo documento que contemple la visibilidad externa, ya que se eliminó del borrador de nomenclatura simple.

El protocolo de enrutamiento para HomeNet será Babel, y hubo una discusión sobre cómo se realizaría la autenticación en Babel. Mientras que algunos en el grupo de trabajo dijeron que bastaría con una mención en las consideraciones de seguridad del documento, Lemon solicitó un análisis de amenazas y una solución a decidirse. De lo contrario, se entretejería diversos mecanismos de autenticación y se perdería la interoperabilidad.

Grupos de trabajo y BoFs

RegExt de Grupo de trabajo o GT: ¿Qué debe de ser primero: los estándares o las políticas?

El GT de RegExt se reunió dos veces en Chicago, experimentando con sesiones separadas durante la primera reunión, para hablar más en profundidad sobre las propuestas en RDAP y EPP. Se presentaron varios resúmenes en la segunda reunión y la discusión principal fue ilustrativa de un problema específico que el grupo sigue teniendo: en muchos casos, el grupo desarrolla mecanismos que dependen de las decisiones políticas de los órganos de interés de la ICANN.

El problema es evidente en -la solución de acceso federado para las consultas RDAP que Verisign ha estado trabajando desde hace un tiempo. La solución se basa en Open ID Connect (sin el estándar del IETF) que permite el registro de las decisiones sobre el acceso basado en autenticación y validación de terceros proveedores. Para la prueba de VeriSign, se trató Googlemail, Paypal y Cz.Nic. Según Hollenbeck, la solución de acceso federado puede ser una opción para permitir el acceso de capas a terceros, como para aplicación de la ley y los propietarios de marcas registradas. La descripción de Hollenbeck para credenciales de la aplicación de ley fueron bastante más simplistas. Sin embargo, dijo que la validación y acreditación podrían ser externalizadas al FBI. La decisión sobre quién es una LEA y quién tiene el derecho legítimo de acceder a los datos es bastante difícil de resolver a escala global.

Hollenbeck reconoció que mientras las tecnologías estuvieran trabajando, quién debe tener acceso a qué es actualmente el tema de una política de desarrollo en un grupo de trabajo de ICANN, "y que aún les falta un largo camino para el establecimiento de políticas". Si bien los operadores de ccTLD podrían tener sus directrices acerca de quién tiene acceso a qué (donde el nuevo Reglamento General de Protección de Datos de la UE es citado como estricto para mantener los

datos personales alejados de la divulgación pública), cualquier cosa que el WG de Regex decida ahora "no puede ser consistente con lo que salga de ICANN después ", dijo Hollenbeck.
Un participante comentó que se deben evitar los bloqueos entre el del RegExt GT mientras espera a ICANN, y por otro lado ICANN diciendo que no podía seguir adelante debido a la falta de un estándar técnico. ¿La pregunta clave aquí es qué debe de venir en primer lugar: el código o la política? Extrañamente, dicha pregunta no se formuló.

Propuestas que se discutieron durante las reuniones

Hablando de una de las tres propuestas de RDAP discutidas más intensamente durante el RDAP Breakout, Hollenbeck dijo que el trabajo de política en ICANN sobre quién recibiría qué datos del nuevo sistema todavía estaba en discusión y tomaría un tiempo considerable en decidirse.
Scott Hollenbeck (VeriSign) presentó todos los borradores que se discutieron en la parte RDAP de las sesiones. No hubo prácticamente ningún interés expresado por los participantes para implementar un método para RDAP que añadiera "búsquedas" utilizando expresiones regulares. Los parámetros de consulta de expresión utilizados regularmente se diferenciaron de la búsqueda de base, y alguna "codificación mágica" tenía que ser utilizada porque las expresiones regulares no eran URL-seguras. (El formato debe brindar soporte de codificación base64url en lugar de codificación hexadecimal para evitar mezclar consultas con direcciones URL de búsqueda). El resultado no fue amigable con la línea de comandos, pero fue probado por VeriSign contra algunos cctlds (no gtlds debido a obligaciones contractuales con la ICANN). La solución dio a los usuarios una "buena lógica booleana", dijo Hollenbeck. Fue posible hacer una delimitación de tasa de acceso, acotó uno de los desarrolladores de Verisign, agregar un enumerador sin-estado o permitir que los parches sean enviados de vuelta (dame los primeros diez de 100). VeriSign declaró que tiene derechos de propiedad intelectual sobre el método, pero Hollenbeck dijo que "es código libre". La capacidad de búsqueda ha sido un tema de discusión controversial en RDAP Como ningún participante demostró interés, Hollenbeck dijo que podría considerar llevarlo al grupo de trabajo como un documento de presentación individual, e informativa (no como un estándar).
Tampoco hubo acuerdo sobre la segunda propuesta, pero sí un cierto interés en trabajar en una "etiqueta de entidad" que permitiera un enlace más fácil de servicio y operador. Se podría adoptar una convención, dijo Hollenbeck, con algún tipo de etiqueta que apuntara al servidor. Esto se crearía sobre una lógica ya existente. Sin embargo, implicaría la creación de un registro de IANA. Una preocupación planteada en este punto por Marcos Sanz, de Denic, fue cómo las soluciones existentes pudieron dar lugar a confusión para los clientes sobre donde mirar y donde no mirar. En Denic, las etiquetas fueron agregadas como prefijo en vez de la solución prevista del sufijo; y ¿qué sucedería si la etiqueta estaría en el medio de la entidad? "Cosas extrañas pueden suceder" dijo Sanz. La discusión continuará sobre este asunto. Las cuestiones discutidas durante las sesiones EPP incluyeron un borrador sobre las tarifas en EPP, una extensión del revendedor (la necesidad fue cuestionada por algunos, el identificador de reventa es un campo opcional en la política consistente de etiquetado y visualización) y una propuesta de protocolo para permitir que un operador tercerizado de DNS pueda actualizar los registros DS de una delegación (una pregunta que se planteó fue "eso está dentro del ámbito del GT?", ya que el tema se ha discutido en reuniones anteriores de DNSOP).
Una propuesta sobre nuevos parámetros de búsqueda "availabilityCheck=1" /"availabilityInformation=1" (Andy Newton Arin/Marcos Sanz Denic) dio lugar a un fuerte rechazo

de Jim Gould. RDAP es acerca de información, no sobre disponibilidad. Newton ofreció que se pudieran consultar diferentes servidores.

Re-chartering: mayores documentos de extensión, ¿informativos o estándares?

El Grupo de Trabajo está por volver a cambiar su charter (lo que es totalmente necesario para trabajar en temas de custodia de documentos (escrow), por ejemplo). El nuevo director de área (y algunos de los participantes) expresaron su preocupación sobre los muchos documentos que fueron procesados y aprobados por un pequeño número de personas. Hasta ahora no parece haber una solución aparente para esta desafortunada situación.
El co-presidente Jim Galvin (Afilias) – quién ha precedido las reuniones desde hace un tiempo a solas debido a la participación remota de Antoin Verschueren – se dirigió a la crítica al anunciar que revisaría la lista de documentos para ver si todos ellos necesitan estandarizarse o si solo podrían convertirse en documentos informativos en su lugar. Con muchos de los documentos que ya han caducado, otra tarea era pedir a los autores a revivir y aclarar la situación. Los documentos de custodio (escrow) elaborados por personal de ICANN (Francisco Arias) también tuvieron que ser revividos.
Documentos publicados: RFC 8056 (mapeo de estados RDAP) además de RFC 8063 (Key Relay). El documento de la fase de lanzamiento está listo para WGLC (Ulrich Wisser es el pastor del grupo).

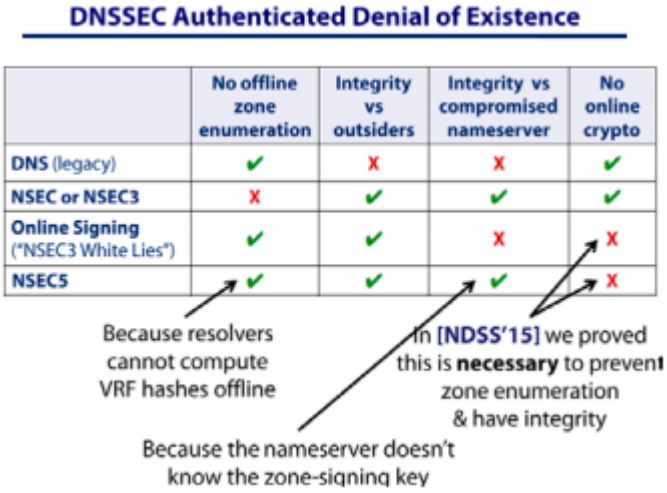
GT de DNSOP: NSEC5, listo los TLDs de uso especial , .alt en la lista de deseos

El GT de DNSOP está analizando un número considerable de documentos. Con cierto alivio, los presidentes clausuraron los debates sobre dominios especiales. El documento de terminología DNS (la última reunión del GT se reunió antes del evento en Praga) y un documento sobre la gestión de la zona de ip6.arpa para IPv6 por Lee Howard (Time Warner Cable) están también cerca de ser finalizados.
Luego de la prolongada discusión sobre los TLDs de uso especial en los últimos años, los presidentes del grupo de trabajo declararon consenso, poco después de la reunión del IETF, en el documento escrito por Ralf Droms, Ted Lemon, Nominum y Warren Kumari, Google. El documento está ahora en camino al IESG. El mismo diferencia entre cinco tipos de nombres:

- aquellos reservados por el IETF para usos técnicos;
- aquellos asignados por ICANN a la raíz pública (de los cuales algunos nombres fueron reservados por IETF con fines técnicos para que aparezcan en la raíz DNS global, por razones relacionadas con el funcionamiento del DNS);
- aquellos reservados por ICANN (para los que no pueden efectuar aplicaciones, por ejemplo ccTLDs);
- aquellos utilizados por otras organizaciones (.int, .gov); y
- aquellos sin utilizar, y por ende disponibles para su asignación a una de las categorías anteriores.

El documento también enumera los problemas de diferenciación entre los distintos "tipos" y deficiencias en la claridad en los procedimientos de asignaciones. Señala, por ejemplo, que no hay "ninguna coordinación formal vigente del proceso entre ICANN y el IETF ya que cada uno sigue con

sus procesos de asignación de nombre respectivo (ver sección 4.1.3). La falta de coordinación complica la gestión de la raíz del Espacio de Nombres de Dominio y podría conducir a conflictos en las asignaciones de nombres [SDO-ICANN-SAC090] ". "No hay [tampoco] ningún alcance explícito en cuanto a qué puede constituir un *uso técnico* [RFC 2860] y lo que no, y tampoco hay consenso dentro de la IETF en cuanto a lo que este término significa".
Como el nuevo Director de Área, Warren Kumari, es un autor, se asignará a otro miembro del IESG para los próximos pasos. Entretanto, la propuesta de agregar un .alt su-TLD como hogar para nombres alternativos DNS que no estén en la raízs (home.alt) llegó a la etapa de última llamada del GT, desencadenando otra ronda de discusión.
NSEC5 es una nueva propuesta presentada a el IETF por la experta en criptografía Sharon Goldberg y los autores de cz.nic, Akamai y Salesforce. Goldberg presentó el concepto en DNSOP y la solución crypto en el área de seguridad del GT. Según Goldberg, la ventaja básica es que permite la no-enumeración de zonas, combinada con la protección de integridad (contra cualquier enemigo, incluso cuando un servidor fue comprometido - ver gráfica). El concepto también sería viable para los escenarios de alto rendimiento, según Goldberg. En Resumen, NSEC5 reemplaza a Sha1 con una función aleatoria verificable (vrf). Documentos sobre el concepto de criptografía y despliegue pueden ser vistos aquí
El despliegue y la necesidad del enfoque fueron cuestionados por los participantes. Algunos advirtieron que pedir ahora a los operadores de DNSSEC que dejaran de usar la negación autenticada de la existencia sólo retrasaría el despliegue de DNSSEC. Algunos lo llamaron una "solución elegante para un problema que no tenemos". La combinación con otros conceptos como "el uso agresivo de caché negativo" también fue cuestionado.

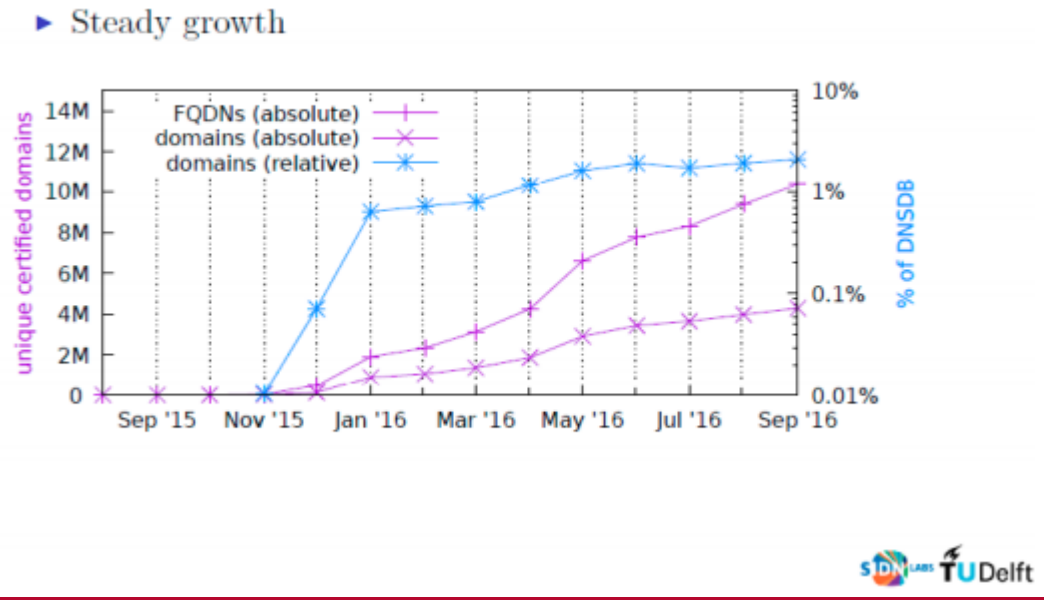


Los documentos que aún están en desarrollo en el grupo incluyen consideraciones operacionales para el transporte DNS a través de TCP, formato de captura para paquetes DNS (C-DNS) y actualización de algoritmos para DNSSEC.

Consideraciones sobre el Protocolo de Derechos Humanos (HPRC)

La campaña "Let's Encrypt" de la EFF es una historia de éxito, según un estudio realizado por investigadores del Centro Nacional de seguridad cibernética en los países bajos, la Universidad de Delft y los laboratorios SIDN y presentados durante el grupo de investigación HPRC. Tras las

revelaciones de Snowden, la tasa de encriptaciones fue claramente en aumento, además de las reacciones en la estandarización (RFC 7258), y los proveedores de sistemas operativos móviles y proveedores de nube que empujan la encriptación por defecto o lo habilitan en cualquier lugar. Actualmente la mitad del tráfico de la web se encuentra cifrado.
Las estadísticas recogidas por el presentador muestran que la campaña "Let's Encrypt", que se centró en la automatización y bajo costo (certificados gratuitos), fue muy utilizado por aquellos con menos incentivos para encriptar – organizaciones y empresas más pequeñas (fuera del Alexa Top 100). Al trazar un mapa de los certificados a direcciones IP, los autores del estudio encontraron que aproximadamente 66.000 entidades han emitido certificados con Let's Encrypt. También es interesante que el 47 por ciento del crecimiento puede atribuirse a tres grandes proveedores de hosting.
El HPRC RG estaba desbordado de presentaciones académicas que resultaron en un debate sobre el uso del tiempo de reunión. Los dos proyectos nuevos sobre el anonimato y la libertad de asociación no pudieron ser discutidos en Chicago. La relación entre estandarización/ingeniería y los derechos humanos parece ser un tema académico de moda.



Destacados IETF/IAB

IAB, preparado para el Grupo de Coordinación de la Comunidad (nueva IANA)

Con la transición de IANA completa, el IAB ha elaborado procedimientos para fijar reuniones para el Grupo de Coordinación de la Comunidad (RFC 8090) y el Comité de revisión de evolución raíz de zona (RFC 8128).

Salientes y entrantes

Terminó su mandato en el IESG en Chicago tanto Jari Arkko como Stephen Farrell (Trinity College).

Terminaron su mandato en el IAB Russ Housely (Vigilsec), Andrew Sullivan (Oracle/Dyn), Ralph Droms y Dave Thaler (Microsoft).

Ingresos por debajo del presupuesto del 2016

El total de ingresos del 2016 del IETF fue de $3.925.501 USD, $410.499 USD por debajo del presupuesto (-9.5%), mientras que los gastos (excepto herramientas de desarrollo) ascendió a $6.354.822 USD, es decir, $147.464 dólares menos de lo presupuestado. Incluyendo el financiamiento del desarrollo de herramientas, ISOC proporcionó $2.574.164 USD a la financiación, de $208.878 USD por sobre el presupuesto de 2016. El resultado general fue mejor de lo que se temía en marzo y se ayudó grandemente al bajar los costos de espacio para reuniones y comidas y bebidas debido a los cambios en valuación de la moneda.

Informes recientes de IAB

Coordinating Attack Response at Internet Scale (CARIS) Workshop Report ("Coordinación de respuesta de ataque a escala de internet") (at theRFC Editor) en el editor RFC
Informe sobre la Internet de las cosas (IoT) Interoperabilidad semántica (IOTSI) Taller 2016
Report from the Internet of Things (IoT) Software Update (IoTSU) Workshop 2016 ("Informe sobre el Internet de las cosas (IoT) Actualización de software (IoTSU) taller de 2016"(en revisión comunitaria, casi terminado)
IAB Workshop on Managing Radio Networks in an Encrypted World (MaRNEW) Report ("Taller IAB sobre la gestión de redes de Radio en un mundo cifrado (MaRNEW)")
Confidentiality in the Face of Pervasive Surveillance ("Confidencialidad frente a la vigilancia omnipresente")
Out With the Old and In With the New: ("Afuera lo viejo, bienvenido lo nuevo") Planning for Protocol Transitions ("Planificación de las transiciones del protocolo") (en revisión comunitaria, casi terminado)
Improving the Public Key Infrastructure (PKI) for the World Wide Web ("Mejorando la infraestructura de clave pública (PKI) de la World Wide Web")

Incoming and outgoing IETF Chairs Alissa Cooper and Jari Arkko