Informe de CENTR

IETF 100

Singapur, 11 - 17 de noviembre de 2017

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

IETF100: «Hacemos que Internet sea mejor... ¿para los humanos?»

En el brindis de la 100ma reunión, la sesión plenaria del IETF escuchó la urgencia de los ingenieros para que se preste atención a las consecuencias sociales de las tecnologías que estaban estandarizando. Se terminó la época en la que los ingenieros de Internet podían despegarse de las responsabilidades de los daños colaterales o abusos de sus productos, según dijo Henning Schulzrinne, profesor en la Universidad de Columbia, participante de larga data en IETF y funcionario en la FCC durante el mandato de Obama.

En el transcurso de un panel de debate especial con Schulzrinne, Monique Morrow, fundadora de la iniciativa *The Humanized Internet* y Jon Murai, padre de la Internet en Japón, Schulzrinne instó a sus colegas a cambiar el autoadjudicado mandato «hacemos que Internet sea mejor» por «hacemos que Internet sea mejor para los humanos». Quizás la revelación más importante de la reunión plenaria de «cumpleaños» del IETF100 fue que las preocupaciones de Schulzrinne sobre las tendencias técnicas despertaron ecos en por lo menos algunos de los participantes.

De herramienta de empoderamiento a herramienta de represión

La idea original de la interconexión de redes como una herramienta de empoderamiento y democratización no resistió el paso del tiempo. Mientras tanto, Schulzrinne dijo que, cada vez más, el objetivo era restringir las comunicaciones, y que la red estaba dando paso a gobiernos autoritarios y sociedades represivas. Mencionó que el trabajo de los ingenieros ya no se limitaba a «poder jugar con cosas geniales».

Debían también considerar las maneras en las que se podría hacer uso y abuso de su tecnología. Morrow recalcó, además, la necesidad de que los ingenieros tengan en cuenta los aspectos éticos. Schulzrinne señaló que la ciberguerra y el *profiling* deberían ser agregados a la lista de desarrollos técnicos no tan positivos. Al mismo tiempo, advirtió sobre la tan debatida «politización» de la Internet.

Indicó también que los ingenieros rara vez podían hacer juicios de valor sobre estos temas, y que, debido a que «*polis*» en su sentido original significa «comunidad de ciudadanos y su gobernanza de manera natural», la Internet debía formar parte del debate político, pero no convertirse en una herramienta para dicho debate.

Schulzrinne describió un amplio espectro al analizar las potenciales tendencias tecnológicas del futuro. El transporte cuántico y/o los proyectos como el Brain Circuits Project (BCP) pueden cambiar el paradigma de «transporte» y dejar obsoleto al TCP/IP. A la vez, las tecnologías han demostrado perdurar mucho en el tiempo, por lo que Schulzrinne piensa que no solo la red se convertirá en el tercer producto básico tras el agua y la electricidad, sino que en 2047, hasta los paquetes de Ipv4 puede que sigan aquí.

De vuelta al punto de partida y a los monopolios

Con respecto a lo económico, Schulzrinne describió la posible situación de que en el 2047 volvamos al punto de partida. En 1986, cuando nació el IETF, existían las operadoras

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

tradicionales de telecomunicaciones. Luego de fragmentarlas, la Internet está una vez más camino a ser dominada por unos pocos y grandes proveedores de plataforma de red/contenido integrados. Recientemente, Geoff Huston había explicado este concepto con mayor profundidad (vea el informe de CENTR RIPE75). Schulzrinne comentó que, a diferencia de los primeros días del IETF, en un mundo de unas pocas compañías gigantes, sería más difícil que los ingenieros que participan en el IETF no cuestionen —como individuos y ciudadanos— las estrategias de sus empleadores.

Cada vez menos operadoras de centros de datos/redes empresariales comprenden, en absoluto, las especificaciones. Debido a que la automatización de la red es una tendencia importante, simplemente compraron *hardware* y *software*. Schulzrinne afirmó que pronto nadie sabría quiénes producen los estándares y dónde.

El IETF sufrió los efectos de estas tendencias de varias maneras. Debió ajustarse económicamente. Habiéndose beneficiado del desvío del dinero liberado por el traspaso de conmutadores de telecomunicaciones a tecnología de Internet menos costosa, el dinero fue redirigido nuevamente e invertido en otros aspectos, y no en la «red» de servicios públicos. El número de participantes podría disminuir y, de hecho, ya ha disminuido.

¿Se marchita el IETF?

Se debatió brevemente la disminución en la cantidad de participantes del IETF en parte del IAOC de la plenaria. Se presentaron 153 personas menos de lo estipulado y presupuestado en el IETF99 en Praga: por lo tanto, la reunión sobrepasó el presupuesto por $ 250.000 dólares estadounidenses. La asistencia paga en el IETF98 en Chicago tuvo un déficit de 105 participantes y el IETF97, de 127. La brecha entre la estimación y las asistencias reales causa un déficit de financiación, que el IAOC aborda mediante llamamientos a la ISOC (vea también la información sobre la reunión IETF en Buenos Aires).

Hace varios años que encontrar nuevas fuentes de financiación para el IETF está en los planes de la dirección. Un enfoque armado por la nueva presidente del IETF y su predecesor fue convocar a nuevos grupos, además de los clásicos proveedores, y traer nuevos trabajos al IETF. Durante la reunión en Singapur, la Directora de Área de Enrutamiento, Alia Atlas, organizó una reunión sobre las actividades de divulgación del IETF, en la que se especificaron varios tipos de actividades. Estas varían desde las muy famosas hackatones (que todavía luchan por encontrar patrocinadores) a nodos remotos especiales (en países como la India).

Jun Murai, panelista en el IETF100, les pidió a los ingenieros del IETF que «saquen de los silos» a los trabajos sobre tecnologías futuras, ya que muchas áreas como la tecnología médica o la agricultura no estaban al tanto de la tecnología que desarrolla el IETF.

La búsqueda de las nuevas opciones para subsanar los déficits de financiación parece ganar más relevancia en vistas del comentario de Schulzrinne sobre que la disminución es una tendencia de los mercados cambiantes.

Durante la plenaria del IAOC, Leslie Daigle, la presidente del IAOC, anunció que para 2018, el IAOC había solicitado que la ISOC pagara un adicional de $ 900.000 dólares para compensar la disminución de ganancias prevista en un millón de dólares (con un presupuesto restante de 7 millones de dólares, y la contribución compensatoria de la ISOC que representaba cerca del 50 por ciento, las cifras finales se decidirán y publicarán tras la reunión del Consejo de la ISOC en

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

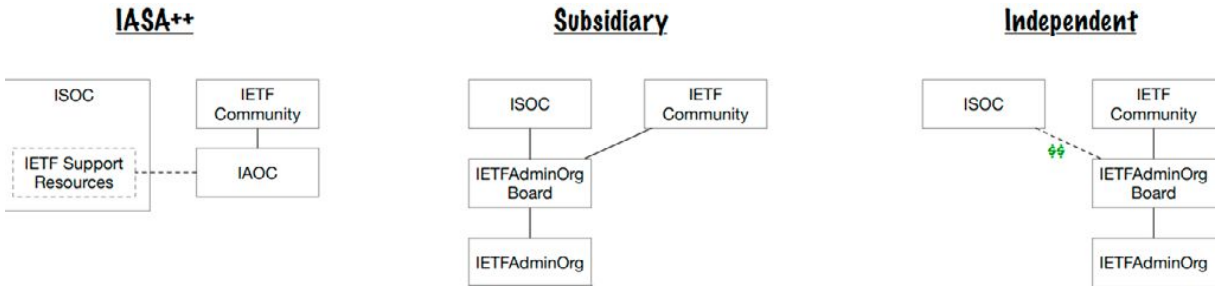
Singapur, luego de la reunión del IETF). Para el 2019, los participantes del IETF se enfrentarán a incrementos más bien pronunciados en las tarifas de inscripción a las reuniones, con más de un 10 por ciento para 2019 y más de un 3 por ciento a partir de 2020. Durante la plenaria del IAOC se debatió la posibilidad de que en el futuro los participantes remotos paguen para participar. La cantidad —pero también los costos— de participación remota va en aumento y sobrecarga el presupuesto de la reunión del IETF.

IASA 2.0: El IETF no busca independizarse de la ISOC, solo busca más dinero

En su reunión en Singapur, el grupo que se encarga de considerar las potenciales reformas del sistema administrativo actual del IETF se mostró en contra de una separación total del IETF y la ISOC. En cambio, dos posturas igualmente fuertes favorecieron, por un lado, un camino evolutivo hacia una estructura IASA 2.0 y, por el otro, una organización subsidiaria/de partes interesadas con más control sobre las decisiones presupuestarias o contractuales, pero aún como un organismo de la ISOC.

Una simple IASA 2.0 podría intentar resolver los problemas principales como la relación entre la ISOC y el IETF. Una subsidiaria, según la presentación de Brian Haberman, podría contar con «su propia cuenta bancaria, reglamento, acta constitutiva, consejo, personal, e identidad empresarial».

Rich Salz (Akamai) compartió una buena ilustración de las tres opciones tras la sesión:



12 años después de la IASA 1.0

La IASA, que incluye el IAOC (el organismo de supervisión de la IASA), el único empleado de la IASA, el IAD, y la Fundación del IETF se desarrollaron y establecieron durante la primera ronda de actualización de estructura del IETF y fueron iniciados por el entonces presidente del IETF, Harald Alvestrand (de Cisco en ese momento) en 2003. Alvestrand impulsó el establecimiento de las estructuras administrativas para satisfacer necesidades de desarrollo y profesionalización. Fue responsabilidad del segundo presidente del IETF escandinavo, Jari Arkko, iniciar la revisión actual: 12 años después de la IASA 1.0.

Existen opiniones encontradas sobre la forma de proceder. El expresidente del IAB, Andrew Sullivan, dijo que el IETF debía decidir si quería ser «adulto» o «maduro». En el otro extremo del espectro, John Levine advirtió que sería un poco difícil para el IETF recaudar una cantidad de dinero similar al que recibía de la ISOC «con tan pocos compromisos».

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

Los problemas de financiación y los cambios en el IETF, pero también en la ISOC por su parte, son el centro del debate. Cuando se inició la actual IASA en 2004/2005, la ISOC todavía era una organización pequeña que contaba con alrededor de 10 empleados, y acababa de recibir el contrato para ser la organización patrocinadora (y beneficiaria) del registro .org, gestionado previamente por VeriSign. Aunque el contrato .org le permitió a la ISOC patrocinar generosamente al IETF (e intervenir cuando el IETF se descarriaba con respecto al presupuesto), la ISOC creció en tamaño y presupuesto, y se convirtió en una organización de cabildeo que cuenta con 100 empleados, que a veces se involucra de más en debates técnicos, en lugar de solo funcionar de hogar para el no incorporado IETF.

Claridad, control presupuestario, nuevas fuentes de financiación

La lista de problemas de la RFC de la IASA 2.0 pone de relieve tanto la falta de claridad (con respecto a la responsabilidad, representación del IETF, autoridad y supervisión del personal y el presupuesto) como también la escasez de recursos y transparencia del actual IAOC. Según el *draft*, los objetivos de los que se habló en Singapur son:

- Proteger la cultura del IETF.
- Mejorar el ambiente de trabajo para la estandarización.
- Definir la relación entre el IETF y la ISOC.
- Sustentar el replanteamiento del modelo de financiación.
- Brindar claridad sobre los acuerdos financieros entre el IETF y la ISOC.
- Aclarar los roles y responsabilidades generales y también apoyar los roles y responsabilidades del personal.
- Redefinir el papel de la comunidad del IETF en relación con las actividades administrativas.
- Definir mejores los requisitos de transparencia.
- Definir un plan de transición.

Kathy Brown, de ISOC, subrayó que la ISOC apoyaría al IETF de todas maneras y previó dejar que el IETF tome la decisión. Al mismo tiempo, Brown señaló que en el pago de cuentas de la ISOC, ciertamente se hacían responsables ante su Consejo. La ISOC es el contratista oficial de los hoteles para las conferencias y el empleador del IAD, que era Ray Pelletier.

Petellier se jubiló el 31 de octubre. El 1 de octubre, Portia Wenze-Danley fue contratada como interina del IAD.

Algunos observan que, dados los vínculos financieros entre ambas organización, no podrán resolverse completamente todos los problemas.

La lucha sobre el cifrado

Debido al creciente cifrado en muchos lugares, TLS, Quic y —poco a poco— el DNS, existe un retroceso por parte de los proveedores/operadoras de *middle boxes* —o, como dicen quienes están preocupados por este retroceso, algunos de estos proveedores/operadoras.

La acalorada discusión en Singapur se concentró en una única presentación (que no pasó por el IESG) en el Área de Operaciones. Recibió el título «Efecto del Cifrado en las Operadoras» [Effect of Encryption on Operators], y muchos críticos la consideran un potencial documento de

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

referencia para que las operadoras soliciten limitaciones (o excepciones) en el cifrado que se incorpora en los nuevos estándares.

Kathleen Moriarty, saliente directora de área de Seguridad, presentó el documento. Luego de muchas críticas, remarcó que recibió el documento por parte de sus colegas directores de área. Moriarty dijo que, en esencia, el documento era un resultado de una RFC pos-Snowden sobre el monitoreo generalizado (RFC 7258), que incluía este reconocimiento: «Hacer que las redes sean inmanejables con el fin de mitigar el monitoreo generalizado (PM, en inglés) no es un resultado aceptable, pero ignorar el PM iría en contra del consenso que documentamos en la presente. Un balance adecuado emergerá eventualmente, ya que se tienen en cuenta instancias reales de esta tensión».

El documento, de poco menos de 50 páginas, describe cómo, mediante el cifrado agregado, las operadoras «pierden» opciones para el monitoreo generalizado, optimización y manejo del tráfico. Incluye una sección especial sobre los problemas de la optimización de la red de movilidad. El capítulo sobre la «respuesta al creciente cifrado y la mirada a futuro» (capítulo 8) favorece una vez más que las «consideraciones para el diseño de protocolos deberían actuar como factor en las funciones de manejo de la red para trabajar en pos del balance». Dejando las preocupaciones de lado, Moriarty advirtió en Singapur que existía el riesgo de que, debido a que el IETF estandariza el cifrado para sus protocolos, no se implementaría completamente. No hubo mucho debate en la reunión del Área de Operaciones en Singapur: la mayoría de los participantes pareció apoyar el documento, incluso cuando uno de los participantes informó que al presentar el documento a los miembros o RIPE, algunos cuestionaron si el cifrado debería ahora considerarse «malo».

El debate principal, en cambio, está tomando lugar en la lista de mails con el más reciente y largo análisis hecho por el experto en privacidad Christian Huitema, quien puso de manifiesto algunas preocupaciones esenciales. Huitema cuestiona el consenso sobre algunos de los mecanismos de funcionamiento de la red —lo que algunos defienden como *proxies* de mejora de rendimiento, en realidad, son *proxies* que empeoran el rendimiento. Según lo que escribió, otro mecanismo dado por perdido es la inserción del encabezado HTTP, que no es una herramienta para el manejo de la red y no debería ni siquiera figurar en el documento. Aunque Huitema reconoce las considerables reescrituras, aún expresa la opinión de que todavía queda trabajo por hacer.

Si bien el documento parece esforzarse para ser publicado como una RFC informativa, siguen vigentes los debates sobre cómo equilibrar el cifrado —el manejo de la red/la solución de problemas/el monitoreo.

Quic continúa debatiendo cómo abordar estas preocupaciones, por ejemplo, en el *draft* «spin-bit». El *spin-bit* en el encabezado de Quic permitirá que las operadoras midan el RTT de extremo a extremo en los flujos de Quic.

Acaba de comenzar, en un documento que busca la aleatorización —«*greasing*»— en el encabezado actual de Quic, un intento para abordar el monitoreo de terceros sin correr el riesgo en cuanto a la osificación.

En el WG de TLS existen al menos dos propuestas que estipulan cómo equilibrar «el mayor cifrado» y las preocupaciones de manejo. La propuesta más reciente es de Cisco, que quiere trasladar el TLS una capa más arriba hacia la capa de aplicación. El mecanismo presentado en

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

Singapur «define un mecanismo para el transporte de registros de TLS en cuerpos de mensaje HTTP entre clientes y servicios». Fueron variadas las reacciones en Singapur. El defensor de la privacidad Daniel Kahn-Gillmore (ACLU) y el presidente de HTTP y copresidente de Quic, Mark Nottingham (Akamai), advirtieron sobre los continuos juegos del gato y el ratón en lugar de impulsar la observancia de *middle boxes* en el nuevo protocolo. Una propuesta más antigua, luego del debate sobre los problemas de centros de datos con TLS 1.3, es de Russ Housley (Vigil Security, expresidente del IETF y parte contratada por la NSA). Propone una «Extensión de Visibilidad de TLS» para abordar específicamente uno de los impactos del (EC)DH «mediante un mecanismo de adhesión que permita que un cliente y servidor de TLS concedan explícitamente el acceso al texto llano de la sesión TLS». Ninguno de estos dos documentos fue adoptado como documento de WG, pero el debate sobre el problema de las *middle boxes* en TLS continúa.

Actividades del DNS y más

Debido a la cantidad de actividades que se están llevando a cabo en relación con el DNS por fuera del WG del DNS, uno podría casi preguntarse si sería necesario revivir el viejo y confiable WG de extensión de DNS (que hace años estandarizaba las DNSSEC, por ejemplo).

DNS sobre HTTPS

Una actividad bastante directa es el trabajo de DNS sobre HTTPS, que, tras ser presentado en el WG Dispatch durante la reunión IETF99, ahora ha tomado impulso en un nuevo y especializado WG. El WG de «consultas DNS sobre HTTPS» (DOH, por sus siglas en inglés) está presidido por Ben Schwarz (Google – empresa que representa uno de los primeros usuarios de una solución DNS sobre HTTPS) y David Lawrence (Akamai), y está abriéndose paso en una lista de problemas originalmente bastante breve, uno de los cuales tiene que ver con las diferentes maneras de cacheo entre el DNS y HTTP.

Los casos de uso básicos para el DNS sobre HTTPS, según la reescritura del texto del *draft* son «prevenir que dispositivos de red en camino interfieran con las operaciones del DNS», en donde la interferencia incluye «la falsificación (*spoofing*) de respuestas del DNS, el bloqueo de solicitudes del DNS, y el rastreo». Para este uso, a los clientes «se les configurará el uso de un servidor DOH como resolutor recursivo por parte de su usuario (o administrador)» para algunas o todas las consultas. Un segundo caso de uso es «permitir que las aplicaciones web accedan a la información del DNS mediante el uso de API existentes en buscadores para acceder a esta sobre HTTP de manera segura y acorde con el Intercambio de Recursos de Origen Cruzado (CORS, por sus siglas en inglés)». Para el segundo uso «el buscador no consulta el servidor DOH ni usa sus respuestas para las búsquedas del DNS fuera del alcance de la aplicación que las usa; es decir, no existe (actualmente) una API que permita que un sitio web envenene el DNS para otros». A diferencia del *draft* sobre DOH, el *draft* sobre el formato de conexión del DNS estaba « utilizando un proxy para consultas del DNS sobre HTTP en lugar de sobre el propio DNS», según indican los autores del DOH, Paul Hoffman (ICANN) y Patrick McManus (Mozilla).

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

¿El DNS como peldaño hacia un sistema Single Sign-on federado?

El DNS como la base para un sistema Single Sign-on federado es el tema principal de una propuesta y prototipo que presentaron Marcos Sanz (Denic) y Vittorio Bertola (Open-Xchange) durante la sesión del WG Oauth. Aunque se base en OpenID Connect, usar el DNS para la «infraestructura de ID Pública» produciría una verdadera interoperabilidad y una mejor forma para que múltiples proveedores ofrezcan identidades de la misma manera. También se lograría más portabilidad, según los autores. Ellos afirman que, de hecho, usar el DNS permitiría «que el usuario, en lugar del proveedor de identidad, se convierta en el único dueño de su identificador mediante la adquisición de un nombre de dominio personal». Varios participantes del WG rechazaron la propuesta, alegando que ya han fallado intentos similares para lograr un sistema de ID federado. Por otro lado, los autores apuntaron a una prueba de implementación en curso del sistema y están planificando presentar la PIDI (Infraestructura de Identidad Pública) y el correspondiente mecanismo de descubrimiento fuera del IETF también (por ejemplo, en el próximo evento de Domain Pulse en Múnich).

¿Se está repensando el DNS (otra vez)?

En vista de todos los desarrollos en torno al DNS, un antiguo participante del IETF y autor, John Klensin, formula una pregunta recurrente en un *draft* individual: ¿es momento de reconsiderar el DNS o pensar en remplazarlo? Klensin explica que, tanto el uso de consultas de tipos múltiples, como la privacidad, o el debate sobre los nombres especiales, el DNS claramente no cumplió con las expectativas que se tenían sobre su funcionamiento. Algunas de las pequeñas curas producidas en los últimos años ilustran justamente esto. El autor remarca que el documento al menos podría ayudar a «simular pensamientos sobre cuán lejos queremos llegar con el DNS existente, para examinar si las expectativas que se pusieron en él ya exceden sus capacidades factibles, y para comenzar el debate sobre un rediseño o alternativas, si es que ya llegó el momento de tomar esa decisión».

Grupos de trabajo (WG)

DNSOP: Una nueva lucha con respecto a un TLD .internal (.homenet), la definición del DNS y más

En el 2017, el WG del DNS publicó 5 RFC en lugar de 7 y, por lo tanto, se ha ralentizado un poco, según el copresidente Tim Wizinski. Si bien hicieron muchos intentos de (re)utilizar el DNS (vea la sección de aspectos destacados, más arriba), los miembros del WG tuvieron una agenda muy ocupada.

Uno de los documentos para el cual el WG espera recibir una amplia revisión antes de llegar a la última llamada (mediados de enero) es la actualización de la terminología del DNS. Se espera que estas definiciones establezcan un estándar y sean utilizadas ampliamente como autoritativas para los conceptos y términos del DNS. Será un documento de estándar propiamente dicho (ya que su predecesor fue informativo).

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

¿.internal en lugar de .homenet?

El WG fue anfitrión de otra edición de la lucha con respecto a un nombre especial TLD luego de que Warren Kumari (ahora director de área del IETF) propuso que el IETF introdujera un TLD «.internal» sobre la base del proceso de Nombres Especiales. Kumari argumentó que se espera que al menos algunas personas que ahora ocupan (mediante *squatting*) los TLD para uso interno (como .home u otros similares) usen dicho TLD. La diferencia con respecto al intento fallido de delegar .homenet, según Kumari, es que .internal fue diseñado para usos mucho más amplios —y la delegación no fue en un momento crítico, ya que ninguno de los protocolos en los que se estaba trabajando dependía de ella. Kumari pidió que el TLD .internal sea asignado a la IANA y que una delegación insegura de DNSSEC sea insertada en la zona raíz: las solicitudes hechas a la raíz deberían encajarse en un *black hole* delegado en iana.org, según el *draft*.

La propuesta de Kumari —similar a la anterior aplicación de .homenet— recibió bastantes objeciones. Andrew Sullivan (Oracle) cuestionó una declaración (en el *draft*) que afirmaba que no existía un proceso para la delegación, y apuntó, una vez más, al proceso de ICANN. David Conrad (ICANN), por otro lado, dijo que no llegaba a comprender por qué, contando con el procedimiento de nombres especiales en el IETF, .internal debía ser dejado a ICANN. Stuart Cheshire (Apple) se quejó porque el IETF seguía ignorando lo que sucede fuera del IETF. No se tomó ninguna decisión con respecto al *draft* y la propuesta de Kumari, pero uno se podría preguntar qué pasaría si .internal tuviera la oportunidad de proceder, dado que homenet fue enviado de vuelta a homenet.arpa.

Aspectos sobre la rotación de llave

También se están llevando a cabo tareas sobre la deferida rotación de llave en el IETF. En Singapur, Geoff Huston presentó una propuesta diseñada para ayudar a obtener un mejor control sobre la distribución de la nueva ancla de confianza. El mecanismo propuesto ubica la medida del lado del cliente. Al usar un conjunto de consultas con etiquetas especiales, los usuarios podrán ser capaces de verificar si una «KSK especial de la Zona Raíz está lista para ser usada como una clave confiable dentro del contexto de la implementación de claves de este resolutor».

Según el *draft*, el proceso centinela hará el test con tres nombres:

- *un nombre firmado válidamente para que las respuestas sobre nombres en esta zona puedan ser autenticadas por un resolutor de validación —un nombre que contenga la etiqueta de más a la izquierda «_is-ta-<tag-index>».*
- *otro nombre firmado válidamente —que contenga la etiqueta de más a la izquierda «_not-ta-<tag-index>.».*
- *un nombre firmado con una firma DNSSEC que no pueda ser validado.*

Las respuestas del servidor de validación permiten determinar el estado de la clave del entorno de resolución del usuario.

o Vnew: Un resolutor de validación de DNSSEC que incluye este mecanismo que ha cargado la clave nominada en su pila de claves confiables responderá con un registro A para «_is-ta», SERVFAIL para «_not-ta» y SERVFAIL para los nombres no válidos.

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

o Vold: Un resolutor de validación de DNSSEC que incluye este mecanismo que no ha cargado la clave nominada en su pila de claves confiables responderá con un registro SERVFAIL para «_is-ta», una respuesta de registro A para «_not-ta» y SERVFAIL para nombres no válidos.

o Vleg: Un resolutor de validación de DNSSEC que no incluye este mecanismo responderá con una respuesta de registro A para «_is-ta», una respuesta de registro A para «_not-ta» y SERVFAIL para nombres no válidos.

o nonV: Un resolutor de validación no DNSSEC responderá con una respuesta de registro A para «_is-ta», una respuesta de registro A para «_not-ta» y una respuesta de registro A para los nombres no válidos.

Si bien emergieron algunas preocupaciones en la lista de mails de las DNSOP sobre si no sería preferible colocar una interfaz de telemetría en el lado del cliente —incluso hubo preocupaciones sobre los posibles problemas de privacidad durante las pruebas mediante sistemas de usuario final—, la mayoría de los expertos apoya una rápida adopción e implementación. Huston dijo que la manera en que se realizaran las pruebas dependía de cómo la implementara cada uno, aunque él tiene previsto confiar en su reconocida y clásica configuración de prueba basada en avisos de publicidad.

En Singapur, David Conrad (ICANN) dijo que prefería una adopción rápida. Para ICANN, el mecanismo podría ayudar a obtener una imagen más clara de la distribución de la KSK de raíz de DNSSEC.

Con respecto al *draft* sobre las consideraciones de seguridad para 5011, las implementaciones de rotación de llaves automáticas, el WG debatió brevemente los comentarios críticos sobre que este trabajo carecía de contribuciones de operadores y no debería ser publicado (Ed Lewis, ICANN). Sin embargo, los participantes del IETF, incluidos los representantes de ICANN, apoyaron la adopción del documento. Durante la última llamada, se planteó una gran pregunta abierta sobre si el tiempo para los intervalos (cuándo es seguro revocar llaves viejas, y demás) debería basarse en intervalos o en tiempo real. Se dijo que la complejidad de la matemática en estos cálculos es un problema.

Un nuevo *draft* que todavía no adoptó el WG tiene que ver con los lineamientos para la validación de DNSSEC.

Más información en respuestas del DNS

Muchos documentos en la agenda del WG tienen que ver con la información adicional enviada en las respuestas del DNS. El WG está analizando los códigos de error extendidos del DNS, lo que permitirá brindar información adicional para las respuestas incorrectas del servidor, indicando alguna ayuda en la causa de fallas del DNS y DNSSEC. Un registro incluirá en una lista varios —y futuros— códigos de error.

Kaznori Fujiwara hizo otra propuesta para brindar varias respuestas en una única respuesta del DNS. Los servidores autoritativos deberían, por ejemplo, añadir un registro de recursos NSEC o registros de recursos A/AAA del nombre de la consulta, incluso si no se pide. A pesar de que muchos en el WG advirtieron que dicho mecanismo incentivaría los ataques de amplificación y DDoS, y que se preferían mecanismos de *pull* en lugar de *push*, Fujiwara señaló que el

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

enriquecimiento de las respuestas ya era práctica común. Brindó un panorama general de las varias propuestas que se habían hecho para estandarizar los mecanismos.

Otros documentos que se debatieron en Singapur incluyeron el muy discutido documento *DNS proxy* redactado por Ray Bellis. El documento sí incluye una sección sobre consideraciones de privacidad, haciendo hincapié en que si «se usa de manera incorrecta, este RR podría exponer información interna de la red». Debido a que la especificación fue diseñada únicamente para el uso de un *proxy* del lado del servidor que estaría bajo el mismo control administrativo que los propios servidores del DNS, «no había ningún cambio en el alcance dentro del cual la información privada podría ser compartida».

Comparison of proposals

Draft	additional answers	multiple responses	aaaa for free	multi qtypes	Accompanying questions
Protocol change	No	No	Yes?	Yes	Yes
Code size	little	some	little	large?	large?
Resolver modification	No	No	Yes?	Yes	Yes
Config complexity	No	Yes	No	No	No
Multiple names	Yes	Yes	No	No	Yes
Multiple types	Yes	Yes	AAAA	Yes	Yes
Multiple rcodes	(NSEC*)	---	---	---	Yes
Negative response	Yes	No	No	Yes	Yes
Fat response if	always	config	always	query	query
Stub support ?	No	No	?	possible	possible
Deployment	easy	easy	gradual	gradual	gradual

Reunión paralela inesperada de Dprive: Pasos de implementación en la privacidad del DNS

Los miembros del WG de DPRIVE se reunieron en Singapur en una reunión paralela por encargo de los miembros del WG para informar sobre el progreso de las implementaciones, debatir el documento sobre rellenado y pedir los nuevos pasos.

Listo: DNS Android sobre TLS del cliente, versión Beta

Eric Kline y Ben Schwartz presentaron las implementaciones para el Proyecto de Fuente Abierta de Android, y Sarah Dickinson (de manera remota) presentó las del Proyecto de Privacidad del DNS. El DNS sobre TLS ahora se puede instalar en teléfonos Android. El código se encuentra en la biblioteca de Android. Una vez descargado, los usuarios tienen tres opciones diferentes para

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

elegir: modo privacidad, modo oportunista, y modo de privacidad apagado. Cuando se lo enciende, el cliente intenta conectar con el resolutor del DNS mediante el DNS sobre TLS y, si el servidor lo habilita, queda cifrado. Se realizó una prueba en vivo en la reunión del IETF en Singapur utilizando el modo oportunista, ya que la red de la reunión del IETF contaba con un resolutor DNS sobre TLS habilitado por Warren Kumari (Google). Con esta implementación, las solicitudes de DNS sobre TLS pueden alcanzar cifras importantes.

Línea de comandos GUI de Microsoft y GUI de Android listas para Stubby

Las implementaciones preparadas por el Proyecto de Privacidad del DNS representan el segundo mayor esfuerzo. Sara Dickinson (Sinodun) anunció el próximo comienzo de una GUI amigable con el usuario para Mac OS —planificada para la semana siguiente a la reunión del IETF. Hubo un considerable interés en el uso del DNS sobre TLS, según informó a partir del último lanzamiento de un cliente de Microsoft, que, por el momento, está basado en la línea de comandos, pero eventualmente se complementaría con una GUI amigable con el usuario.

Las diferencias entre las implementaciones del Proyecto de Privacidad de Google y el del DNS yacen principalmente en el grupo preestablecido de resolutores habilitados para DNS sobre TLS de este último, mientras que la implementación de Android simplemente intenta utilizar el resolutor recursivo que se encuentre a mano. Otra diferencia es que para sus implementaciones, Dickinson eligió ya implementar el rellenado (*padding*), mientras que Google/Android no lo ha hecho hasta ahora.

Última llamada del grupo de trabajo para la aprobación: Entre las consideraciones sobre la latencia y la seguridad

Alexander Mayrhofer (nic.at) presentó el *draft* pendiente sobre rellenado (*padding*), y explicó el trasfondo sobre la elección de 128 bits para el cliente y 426 bits para el servidor. La elección se basó en un análisis matemático hecho por Daniel Kahn-Gillmore (Unión Americana de Libertades Civiles, ACLU). Mayrhofer solicitó más comentarios sobre la carga adicional resultante de 300 a 400 bits. Esta elección bastante «generosa» podría representar un cambio significativo en la latencia, especialmente para los proveedores que conectaron dispositivos en redes *edge* y con centenares de millones de solicitudes por día (lo que resulta en la pérdida de 300 bits por cada par de cientos de millones de bits). Dijo que una elección más conservadora también sería posible. Si bien existía la necesidad de una mayor investigación académica sobre las bases matemáticas, los miembros del WG presentes y el presidente del WG, Tim Wicinksi, acordaron seguir adelante con la última llamada del WG. Demorar más la decisión podría resultar en implementaciones que elijan distintas políticas de rellenado. Dichas diferencias en el rellenado podrían terminar ayudando a identificar la fuente del tráfico cifrado.

Dprive se reunirá durante la próxima reunión del IETF en Londres y finalmente comenzará a hablar sobre la reformulación del acta constitutiva para considerar asegurar el camino entre el resolutor y el servidor autoritativo del DNS. Los participantes de la reunión paralela en Singapur acordaron livianamente planificar una suerte de reunión interina antes del próximo IETF, ya sea de manera remota o paralelamente a la segunda edición del Taller de Privacidad del DNS en el Simposio de Seguridad de Redes y Sistemas Distribuidos (NDSS, por sus siglas en inglés) el 18 de febrero de 2018.

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

El WG necesita un nuevo copresidente, ya que Warren Kumari se retiró del cargo.

DNSSD: Impulsando drafts y hablando sobre privacidad

Luego de bastantes años de estandarización, el WG de DNSSD ha comenzado a considerar las implicaciones para la privacidad que conllevan la oferta de servicios, el descubrimiento de servicios, y el uso de servicios. La información filtrada incluye nombres de *host*, parámetros de red y también la descripción más detallada de instancias de los servicios correspondientes. El descubrimiento en *hotspots* públicos puede causar problemas graves de privacidad, según un *draft* actual redactado por Christian Huitema y Daniel Kaiser, de la Universidad de Constanza.

El *draft* de Huitema y Kaiser propone una solución en la que los *hosts* descubren instancias de Private Discovery Service vía DNS-SD, mediante el uso de formatos especiales para proteger su privacidad en una primera etapa. En el segundo paso, los *hosts* directamente consultan estos servidores de descubrimiento de privacidad vía DNS-SD sobre TLS con un secreto compartido en pares necesario para el establecimiento de la conexión. Un *draft* sobre el emparejamiento seguro "mediante el acuerdo de un secreto y la verificación manual de la autenticidad del secreto utilizando una cadena de autenticación corta (SAS, por sus siglas en inglés)" se puede encontrar aquí, y un *draft* complementario sobre problemas de emparejamiento, aquí.

En Singapur, Stuart Cheshire (Apple), uno de los principales autores del WG (también autor de un documento «guía» sobre las generalidades del DNSSD), presentó un borrador que intenta compilar los varios aspectos de privacidad del DNSSD que los autores podrían considerar, dependiendo de las características de sus respectivos *drafts.* Los objetivos por tener en cuenta (y por evaluar acorde a la situación y eficiencia del protocolo), según Cheshire, son la autenticidad y la integridad, la confidencialidad, el anonimato y la resistencia en contra de varios tipos de ataques (ataques de diccionario, rastreo, relacionamiento entre mensajes (*message linking*) y negación de servicios).

En Singapur, Cheshire expresó su opinión sobre que un *draft* actual redactado por Huitema y Kaiser no alcanzaba a cubrir el abanico completo de problemas. Presentó una lista más extensa de trabajos realizados con respecto a los mecanismos de privacidad del DNSSD. Incluyó varias tecnologías de Apple, como la opción de contactos de modo único para el establecimiento de la conexión en Apple AirDrop, el mecanismo de Apple HomeKit para «encontrar tus accesorios del inicio». Se puede encontrar un trabajo similar en los accesorios de Google Nest (red en malla IEEE 802.15 4) y el dotdot de Zigbee. Cheshire también habló sobre dos proyectos aún confidenciales que están en curso y mencionó una patente que se le acaba de conceder a un proyecto de Apple hecho por él mismo, que había abandonado cinco años atrás. Aún no ha habido declaraciones sobre DPI, pero sonó como si Cheshire, al menos, hubiera querido recalcar el temprano interés de Apple (¿y/o crédito?).

Un documento que pronto se publicará como RFC, actualmente pendiente de resolución ante el IESG, versa sobre un «Proxy de descubrimiento para el descubrimiento de servicios basado en el DNS multicast (Discovery Proxy for Multicast DNS-Based Service Discovery)». Esta RFC planificada hace el intento de combinar la facilidad del uso del DNS Multicast para el descubrimiento de servicios en una red local con la eficiencia y adaptabilidad del clásico DNS Unicast. El nuevo *proxy* de descubrimiento utiliza el DNS Multicast para descubrir Registros DNS Multicast en su enlace local y hace visibles a los correspondientes registros DNS en el espacio de nombres del DNS Unicast. Aquí es donde entran las ideas sobre la arquitectura del nombrado

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

en el DNSSD, y mucho más, junto con Homenet. El enfoque mitiga los problemas que emergen en redes más grandes con enlaces múltiples (entre los cuales no se propagan los del DNS Multicast).

En línea con la futura RFC, el mecanismo básico para el *proxy* de descubrimiento es:

«De manera simplificada, se elige un nombre de DNS descriptivo para cada enlace en una organización. Al usar un registro NS del DNS, la responsabilidad de ese nombre DNS se delega al Proxy de Descubrimiento que está físicamente anexado a ese enlace. Ahora, cuando un cliente remoto realice una consulta Unicast para un nombre que entre dentro del subdominio delegado, el mecanismo de delegación del DNS normal resulta en una consulta Unicast que llega al Proxy de Descubrimiento, ya que se declaró autoritativo para esos nombres. Ahora, en lugar de consultar un archivo de zona textual en el disco para descubrir la respuesta a la consulta, como lo haría un servidor de DNS tradicional, un Proxy de Descubrimiento consulta su enlace local, utilizando el DNS Multicast para encontrar la respuesta a la pregunta».

Según varios miembros del IESG, los cambios necesarios incluyen un análisis más profundo de los riesgos de seguridad y la eliminación del reclamo de DPI de Apple, que fue incorporada en el documento dentro del punto 10. Los reclamos de DPI, usualmente, no entran en los textos de las RFC.

Un documento sobre las notificaciones *push* del DNS está también camino al IESG y a la última llamada. Permite a los clientes actualizarse sobre los cambios en los registros del DNS sobre la suscripción no vinculada a una solicitud del DNS.El *draft* sobre las notificaciones *push* depende de la conclusión de la señalización de la sesión del DNS, incorporada en un *draft* sobre DNS *stateful*. Permitirá reducir la señalización de sesión por mensaje introduciendo TLV para manejar los tiempos muertos e interrupciones de las sesiones del DNS (vea las DNSOP). El *draft* sobre las notificaciones aguarda la finalización del *draft* sobre la señalización de la sesión del DNS que incorpora un estándar camino a la última llamada estimada para diciembre del 2017.

Finalmente, el DNSSD también captó el interés del WG sobre el «Modelo y Enfoque Integrados para la Red Autonómica (Autonomic Networking Integrated Model and Approach [ANIMA])». Según su carta constitutiva, el objetivo principal para el WG es «desarrollar un sistema de funciones autonómicas que lleven a cabo las intenciones del operador de la red sin la necesidad de un manejo detallado de bajo nivel de dispositivos individuales». Para este tipo de automatización de la red, también se necesita el descubrimiento de servicios.

Toerless Eckert (Huawei) presentó brevemente en Singapur el trabajo realizado sobre descubrimiento, sincronización y negociación, incorporado en un *draft* sobre un «Protocolo Genérico, Autonómico y de Señalización» (GeneRic, Autonomic, Signalling Protocol [Grasp]). Grasp «habilitará nodos autonómicos y agentes de servicios autonómicos para descubrir pares de manera dinámica, sincronizar sus estados mutuamente, y negociar la configuración de parámetros uno del otro», según indica el *draft*. Grasp reconoce al DNSSD como un posible mecanismo de descubrimiento para algunas partes, especialmente para los servicios de la capa de aplicación.

Brian Carpenter, uno de los autores de Grasp, subrayó que en el futuro podría ser necesario contar con un espacio de nombre de la IANA especial para Grasp —así que, posiblemente,

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

además del *draft* sobre home.arpa en curso en *homenet*, exista en el futuro un debate similar para otro *draft*.

Ted Lemon, autor de varios *drafts* de Homenet (incluso el *draft* sobre la Arquitectura de Nombrado Simple) debatió brevemente el enlace de los WG de DNSD y Homenet durante la sesión de DNSSD. En esencia, Homenet fue un caso de uso del DNSSD, según mencionó Lemon. Solo carecía del manejo profesional vigente en los entornos del DNSSD, que han sido conducidos por Stuart Cheshire, de Apple, en primera instancia.

Cheshire y Lemon fueron los únicos participantes, según el primero, en el primer grupo de DNSSD dentro de la Hackaton del IETF100. Cheshire dijo que tenía previsto postularse para otro lugar durante el IETF102.

Homenet – modelo de usuario o ISP

Los trabajos sobre Homenet avanzan lentamente. A pesar de que el *draft* sobre la introducción de home.arpa está en la lista de espera del editor de RFC, y Babel como protocolo de enrutamiento va muy avanzado, se produjo un debate importante sobre los posibles modelos para la implementación y brechas prácticas en la arquitectura Homenet.

En línea con la presentación de Jordi Palet (Consulintel.es), experto en el IPv6, Hans Liu (Dlink) confirmó que hasta ahora no se han implementado los protocolos Homenet en enrutadores caseros. Ted Lemon reconoció que podría existir la necesidad de incluir a homenet en los enrutadores para permitir la implementación, además de los pasos de exploración dados por los miembros del WG y algunos *geeks*.

Se le consultó al WG si homenet debería implementarse solamente en enrutadores comerciales de alta gama o también para los enrutadores ISP. El WG expuso las ventajas y desventajas de los conceptos «un enrutador homenet ISP amigable» contra «mi enrutador es mi castillo». Varios apuntaron a que no había mucho incentivo para que los ISP ofrecieran funciones homenet, incluso, por ejemplo, el puenteo entre varias redes en una red homenet. Hacer que el ISP sea el gestor de las funciones homenet podría causar problemas desde el punto de vista regulatorio, gracias a la referencia de un participante al Reglamento General de Protección de Datos (GDPR) de Europa. Si, en cambio, fueran los usuarios los que usen homenet, quedaría mucho trabajo por hacer, ya que el enfoque «mi enrutador/hogar es mi castillo» aún está limitado solo a los *geeks*.

Sobre la arquitectura de homenet, Andrew Sullivan (Oracle) señaló vacíos en el documento actual que hacía que varias características fueran de implementación imperativa, por ejemplo, la delegación segura y DNSSEC, pero no explicaba en sus especificaciones cómo esto se llevaría a cabo. Ted Lemon y Stuart Cheshire argumentaron que el WG había estado en duda con respecto a permitir una arquitectura de nombrado homenet propiamente dicha, así que se eliminaron los aspectos más complicados. Durante una conversación sobre la seguridad de homenet, Lemon remarcó que la delegación segura, DNSSEC y otros aspectos serían más sencillos con un nombre DNS global.

El documento sobre la arquitectura de nombrado simple de homenet cubre «la publicación local de nombres, así como también un servicio de resolución de nombres para nombres locales y

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

globales para dispositivos conectados a homenet», pero no cubre DNSSEC o un nombre DNS global, que fue el tema de un *draft* anterior.

Los mecanismos de seguridad y el establecimiento de la confianza serán los nuevos temas, lo cual también se debatió en el WG de Babel.

La próxima reunión del IETF tendrá lugar en Londres del 17 al 23 de marzo de 2018.

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