INFORME IETF 91

Honolulu

10-15 Noviembre de 2014

Monika Ermert
para

CENTR &
LACTLD

Edición en castellano
actualizada por
Hugo Salgado (.cl)

LACTLD agradece la colaboración de CENTR por los aportes fundamentales para el financiamiento de la iniciativa, así como el apoyo de ISOC y la contribución de Hugo Salgado. Para acceder a la versión en inglés de este informe: https://centr.org/system/files/share/centr-report-ietf91-20141205.pdf

LACTLD
Latin American and Caribbean ccTLDs Organization

Destacados

Debate acerca de la transición de la IANA. No hay necesidad de realizar cambios por ahora

Desde el punto de vista procedimental, el IETF está cerca de completar sus aportes al Grupo de Coordinación de la Transición de la Gestión de la IANA (ICG por sus siglas en inglés). Dicho aporte será realizado en el formato habitual: un documento RFC (pedido de comentarios). La reunión en Honolulu posibilitó una última conversación cara a cara acerca de la respuesta del IETF a la convocatoria de la NTIA (Oficina Nacional de Telecomunicaciones e Información de los EE UU) antes de que aquel presentara su respuesta al ICG en forma de RFC.

El documento, que debía completarse durante la semana del IETF, fue evaluado una vez más en la lista de correos del IETF después de la reunión. Ahora ya ha sido enviado al IESG (Grupo de Dirección de Ingeniería de Internet), según el procedimiento habitual con RFCs, y el IESG pide que se entreguen las declaraciones finales antes del 15 de diciembre. Una vez que el IESG lo apruebe y el editor de las RFCs lo edite y le asigne un número, se lo entregará al ICG, que espera los aportes de distintos "clientes" de la IANA para el 15 de enero.

Los servicios prestados por la IANA, gestionada por ICANN, al IETF incluyen la administración del registro de números de protocolo y el TLD .arpa.

¿Negociar listas de deseos?

Es obvio que todavía hay cierta incertidumbre en relación con la elaboración final de la propuesta de gestión de la IANA una vez que las distintas comunidades hayan decidido cuál es su modelo preferido. Los participantes en la reunión en Honolulu consideraron la posibilidad de que el Comité de Supervisión Administrativa (IAOC por sus siglas en inglés) tenga que seguir "negociando" una propuesta conjunta con los otros clientes de la IANA (Registros Regionales de Internet, ICANN). Bob Hinden, miembro del IAOC, advirtió que "negociar" la postura de la comunidad sería, como mínimo, difícil.

Scott Bradner, participante desde hace mucho tiempo, recomendó que los próximos pasos sean evaluados por los presidentes del IETF y el IAB (Consejo de Arquitectura de Internet), quienes están a cargo de representar los intereses del IETF, con el IAOC como respaldo. Una vez aprobado formalmente, el RFC debería ser la piedra angular de la postura del IETF. A la vez, el miembro del IAOC Tobias Gondrom definió una "lista de deseos" que permitiría a los miembros del IAOC (y a los presidentes del IETF y del IAB) renunciar a las cuestiones menos importantes y defender las más relevantes.

Russ Mundy (Sparta y miembro del IGC) explicó que no esperaba que el IGC combinara las distintas propuestas en un texto de compromiso si hubiera diferencias. Pero la miembro del ICG Alissa Cooper, también miembro del IAB, no estuvo de acuerdo: declaró que el ICG enviaría una sola propuesta a la NTIA, no tres.

Falta de confianza en ICANN

Si bien el IETF/IAB, de manera similar a los RIRs, aboga por la realización de cambios mínimos a la gestión actual de la IANA, las preguntas de varios participantes en el GT del Plan de la IANA mencionaron propuestas alternativas frente a un posible fracaso de ICANN como operador de la IANA. Varios participantes mencionaron la preocupación de que ICANN podría "perder el control" al desaparecer la vigilancia por parte del gobierno de Estados Unidos.

Los problemas mencionados durante el debate fueron los siguientes:

- ICANN podría cobrar por prestar los servicios de la IANA al IETF;
- ICANN podría tomar posesión de IANA.org (lo cual generaría un problema cuando cambie el operador para el registro de protocolos);
- ICANN podría cuestionar la función del IETF como autoridad para .arpa (o su autoridad sobre los dominios especiales).

Randy Bush, de Internet Initiative Japan, advirtió que ICANN es una de las organizaciones "menos transparentes y responsables" y que tiene "más abogados que nosotros protocolos". Se trataron la posibilidad de cambiar de operador, la necesidad de planificar costos si ese cambio se producía y la titularidad de la IANA. Brian Dickson (que trabaja para Twitter) recomendó considerar la posibilidad de que el IETF controle ICANN y mantenga algunas tareas centrales dentro del IETF (la zona raíz).

¿Separar a ICANN de la política de nombres?

Considerando el nivel de desconfianza hacia ICANN y, aún más, la desconfianza en la estabilidad política del sector de nombres, hubo al menos una exhortación a considerar la posibilidad de separar más las tareas del IETF de ICANN. Esta organización podría terminar "en el centro de una guerra cibernética mundial por necesidad, porque el nombre es un punto de control para Internet", afirmó Phil Hallam-Baker, de Comodo. Sería bueno que el IETF estuviera totalmente escindido de estos argumentos. Antes que la titularidad de la IANA, lo principal es la estabilidad de los registros del IETF. Por ahora no se debatió la separación de funciones o una ruptura con el actual modelo de la IANA, y la separación de funciones tampoco es parte del aporte preliminar del IETF.

Documento preliminar de la respuesta al pedido de propuestas del Grupo Coordinador de Internet sobre registros de parámetros de protocolos de la IANA - Link

El IETF enumera sus tareas vinculadas con la IANA como sigue:

- registros de uso especial en relación con los nombres de dominio [RFC6761];
- especificación del protocolo del DNS;
- especificación del requisito mínimo para servidores raíz [RFC2870], que está siendo evaluado;
- consultas con los RIRs acerca de la evolución de la arquitectura de enrutamiento;
- papel en la formulación de políticas relacionadas con el espacio de direcciones de IP y el espacio de números AS [RFC7020],[RFC7249], direcciones locales únicas (ULAs) [RFC4193];
- manutención de subregistros para asignaciones especiales de IPv4 e IPv6 [RFC3307], [RFC5771], [RFC6890];
- elaboración de estándares que podrían influir sobre los RIRs y los proveedores de servicios.

La obligación de permitir un posible cambio de operador de la IANA se trata en el documento final. En relación con los posibles problemas de derechos de propiedad intelectual vinculados con la IANA, el documento solo destaca la necesidad de que el registro de protocolos sea de dominio público.

Los aspectos centrales de la RFC son:

> *No hace falta realizar cambios sustanciales. En los años que pasaron desde la creación de ICANN, el IETF, ICANN y el IAB han creado conjuntamente un sistema de acuerdos, políticas, y mecanismos de supervisión que cubre todas las necesidades. Este sistema funcionó bien hasta ahora, sin involucramiento de la NTIA en su operación. Por lo tanto, no hacen falta nuevas organizaciones o estructuras.*
>
> *(...)*
>
> *La comunidad del IETF está satisfecha con el acuerdo actual con ICANN. El RFC 2860 sigue vigente, y ha sido muy útil para la comunidad del IETF. El RFC 6220 establece una descripción adecuada de servicios y requisitos.*
>
> *Sin embargo, en ausencia del contrato de la NTIA, pueden ser necesarios algunos ajustes para asegurar que se satisfagan las expectativas de la comunidad del IETF. Esas expectativas son las siguientes:*
>
> *Los registros de parámetros de protocolos son de dominio público. La comunidad del IETF prefiere que todas las partes relevantes reconozcan ese hecho como parte de la transición.*

Es posible que, en el futuro, la operación de los registros de parámetros de protocolos sea transferida de ICANN a otro(s) operador(es). La comunidad del IETF prefiere que, como parte de la transición de la NTIA, ICANN reconozca que cumplirá con las obligaciones establecidas en C.7.3 e I.61 del actual contrato de funciones de la IANA, acordado entre ICANN y la NTIA [NTIA-Contract] para lograr una transición sin obstáculos a otro(s) operador(es), si fuera necesario. Además, si dicha transición se produce, la comunidad del IETF espera que ICANN, el IETF y el/los nuevo(s) operador(es) trabajen juntos para minimizar la disrupción del uso de los registros de parámetros de protocolos u otros recursos localizados actualmente en iana.org.

Sobre el tema de la jurisdicción, el documento preliminar de IETF establece lo siguiente: "Este mecanismo es mundial por naturaleza. El acuerdo actual no especifica la jurisdicción".

Soluciones a la privacidad del DNS: soluciones determinadas por distintos intereses

Se inició la tarea del nuevo Grupo de Trabajo dprive

El trabajo sobre la privacidad del DNS arrancó con un nuevo grupo de trabajo dedicado, dprive, que inició oficialmente su tarea justo a tiempo para tener su primera reunión en Hawai. Si bien los avances en el debate sobre la privacidad del DNS parecen haberse lentificado durante el IETF en Toronto, el GT sobre dprive está revisando la lista de propuestas alternativas presentadas por varias partes.

El acta constitutiva adoptada por el GT limita la primera tarea a la discusión de cuestiones vinculadas con la privacidad entre el servidor stub y el resolvedor. Básicamente, hay dos líneas de trabajo diferentes, como explica Stephane Bortzmeyer, de AFNIC, autor del planteamiento del problema. Una busca la minimización de los datos, y la otra introduce la encriptación para el tráfico del DNS.

Despojar las consultas de datos innecesarios

La minimización de datos, para la cual Bortzmeyer presentó un documento preliminar al DNSOP, implica enviar solo lo necesario en una consulta que recorre el árbol del DNS. Las consultas completas (www.example.com) no tienen que enviarse desde un resolvedor recursivo a la raíz, ya que la respuesta resultará, de todos modos, en una delegación hacia .com.

Mientras que una de las tendencias en el debate es enviar "menos que antes" y solo lo que sea "absolutamente necesario para recibir una respuesta", la otra va en la dirección opuesta. Según la propuesta de varios autores de Google y Akamai, lo mejor es enviar más información para permitir la elaboración de respuestas localizadas. El documento preliminar introduciría "una opción EDNS0 para permitir que los resolvedores recursivos, si están dispuestos, reenvíen detalles sobre la red de origen de la cual proviene la consulta cuando hablan con un servidor de nombre de autoridad". Sin embargo, este documento no fue presentado en Hawai. Es evidente que

algunos modelos de negocios y empresas, que están interesados en el análisis y el mayor uso (comercial) de "big data" de DNS, no favorecen la minimización.

La encriptación del tráfico del DNS

En cuanto a la encriptación del tráfico del DNS, siguen apareciendo nuevas propuestas. Una de ellas está siendo puesta a prueba por un grupo de investigadores de la Universidad de California del Sur y de VeriSign Labs: DNS sobre TLS. (Esta incluirá el pasaje de tráfico de UDP a tráfico de TCP para el DNS. Se presentó una propuesta sobre este tema durante el GT de DNS, véase más abajo.)

Para la variante DNS sobre TLS presentada por el grupo VeriSign Labs/USC, los clientes y servidores indicarán sus preferencias en el encabezado (véase el documento preliminar de la propuesta):

"Clientes y servidores indican su apoyo a DNS-sobre-TLS y su deseo de utilizarlo a través de un bit en el campo Flags de EDNS0 [RFC6891] OPT meta-RR. El bit 'TLS OK' (TO) se define como el segundo bit de los bytes tercero y cuarto de la porción 'RCODE extendido y flags' del EDNS0 OPT meta-RR inmediatamente adyacente al bit

'DNSSEC OK' (DO) [RFC4033] (...)"

Para "minimizar" la exposición de los datos, los autores recomiendan enviar una consulta ficticia estándar para inicializar la comunicación de TLS bajo la forma de "(RD=0, QNAME='STARTTLS', QCLASS=CH, y QTYPE=TXT ('STARTTLS/CH/TXT')". Luego del pasaje exitoso por TLS, las conexiones pueden ser encriptadas y, así, estarían protegidas de los espías. Dado que solo hace unos meses se dijo que el DNS era un protocolo público y difícil de modificar, esta opción será complicada de desarrollar.

Análisis del costo en tiempo

No obstante, existe cierta preocupación, que no es menor en el caso de grandes proveedores de servicios en DNS. Estos señalan, particularmente, la latencia agregada (debido a viajes de ida y vuelta adicionales) y los altos requisitos de ancho de banda para operar el DNS. Según un proveedor grande de DNS, el costo aumentaría significativamente y haría falta más hardware.

VeriSign Labs y USC trataron de calcular el "costo" del tiempo, y dijeron que estaban seguros de que sería razonable. Las pruebas realizadas y sus resultados se explican en detalle en un trabajo que sostiene que "la instalación del TCP y la resolución del DNS durarían menos de 1 ms". La instalación de TLS es más cara, 8 ó 26 ms, y varía según la implementación, mientras que la reanudación sería diez veces más rápida que la instalación completa. Resumiendo, VeriSign Labs/USC estiman que "la latencia de punta a punta desde TLS al resolvedor recursivo es solo aproximadamente un 9% más lenta cuando se utiliza UDP al servidor de autoridad, y un 22% más lenta con TCP al servidor de autoridad".

También rechazan la noción de que "se necesita hardware nuevo", y sostienen que "un resolvedor recursivo grande puede tener 24.000 conexiones activas, que requieren más o menos 3,6 GB de RAM adicional". Sin embargo, el grupo subrayó que era necesario reducir los gastos generales durante la implementación a través de "la canalización de las consultas, permitir respuestas desordenadas, la reanudación de la conexión de TLS y la definición de timeouts adecuados valor plausible de tiempo muerto".

Espacio de soluciones

DNS sobre TLS no es en absoluto la única solución, y, además, es bastante anterior a dprive. Ya fue una opción para los servidores Nlnet Unbound, aunque se utilizó un puerto diferente.

Se hicieron otras dos presentaciones en Hawai. Paul Hoffmann (Internet Mail Consortium) introdujo brevemente dos o tres posibles abordajes del DNS encriptado:

- encapsular las consultas del DNS en pedidos http (y las preguntas como respuestas http, p.ej., https://8.8.8.8/.well-known/dns-in-https/TN4AAAABAAAAAAAAB2V4YW1wbGUDY29tAAABAAE=) como pedido uri, y
- DNS sobre TCP utilizando ALPN para el transporte (puerto 443 en lugar de 53),
- o utilizando un puerto completamente nuevo.

A la vez, Hoffmann sostuvo que DNS sobre TLS podría ser una opción racional. La posible ventaja de sus propuestas sería que podría eludirse la inclinación de los dispositivos intermedios a rechazar TLS sobre el puerto 53.

Philip Hallam-Baker está preparando otra proposición por escrito que, aparentemente, privilegia UDP, pero sin DTLS. Declaró que los elementos principales de su propuesta son ciento por ciento de conectividad, un desempeño igual al actual, transacciones sin estados precedentes y sin clave pública, eludir interferencias, eliminación de los ataques de amplificación y de relay, tamaño escaso y baja complejidad, confidencialidad y la habilitación de lo que él llama "DNS depurado".

Muy anterior – de hecho, pre-Snowden – es el conjunto de programas DNSCrypt y DNSCurve, que encriptan el tráfico DNS desde el resolvedor stub hasta el recursivo, y del recursivo al de autoridad, utilizando algoritmos de curva elíptica. Estos programas no emplean una gestión jerárquica y centralizada de la distribución de claves. Diseñado originalmente por Dan Bernstein en 2008 para responder a inquietudes vinculadas con el DNSSEC, este conjunto de programas no ha sido adoptado por los operadores del DNS.

Si bien reconocen que los protocolos abordan las mismas inquietudes relacionadas con la privacidad que DNS sobre TLS, VerisignLabs/USC critican el hecho de que no responden al problema de los ataques distribuidos por denegación de servicio (DOS por sus siglas en inglés), algo que DNS sobre TCP y TLS aspira a resolver junto con la cuestión de la privacidad.

Finalmente, parece que habrá nuevas propuestas. Una fue posteada como documento preliminar por Hosnieh Rafiee, ingeniero en Huawei Technologies Düsseldorf en Munich: "CGA-TSIG/e: Algoritmos para la autentificación segura de DNS y la confidencialidad de DNS opcional". Rafiee no pudo conseguir la visa para viajar, pero puede ser que presente su propuesta en la próxima reunión.

Próximos pasos: ¿requisitos o documento matriz?

Todavía no se ha tomado una decisión respecto de las distintas propuestas. Por ahora, el GT empezó a analizar otro documento general: un documento preliminar o matriz sobre requisitos que permita evaluar los elementos a favor y en contra de cada solución. Por cierto, VeriSign Labs/USC están más avanzados, porque pueden referirse a un código (preliminar) que funciona. Allison Mankin, de VeriSign, y John Heidemann, de USC, también presentaron el documento de investigación más amplio, que avanza en la descripción de los requisitos y cómo fueron abordados por cada propuesta. El grupo USC/VeriSign muestra una cierta parcialidad hacia su propia alternativa.

IAB: ¡Abandonemos los textos sin encriptar en la red, por favor!

Al final de la semana del IETF, el Consejo de Arquitectura de Internet publicó una declaración sobre confidencialidad en la red, que recomienda a los diseñadores e implementadores de protocolos que utilicen el cifrado en todas las capas de la pila de protocolos: desde el transporte a los programas. La declaración contiene más información que el documento preliminar anterior del director del Área de Seguridad, Stephen Farrell ("El monitoreo generalizado es un ataque"), pero es más breve y algo más directa en sus recomendaciones: "El IAB cree ahora que es importante que los diseñadores, programadores y operadores de protocolos conviertan al cifrado en la norma para el tráfico de Internet. La encriptación debería ser autenticada siempre que fuera posible, pero incluso los protocolos que brindan confidencialidad sin autentificación son útiles frente a la vigilancia generalizada que se describe en el RFC 7258".

Cuando se le preguntó por qué el IAB decidió utilizar "debería ser autenticada" y dejó lugar para las "excepciones" a la norma de cifrado, Russ Housley, presidente del IETF, afirmó que había habido un largo debate en el IAB. La razón por la cual se permitió cierta flexibilidad es que, de lo contrario, algunos protocolos (como Secure Neighbor Discovery, o SEND) dejarían de funcionar. Housley declaró que el IAB publicará pautas que expliquen la lógica que justifica las excepciones y las expectativas respecto de ellas. ¿Cuán considerable será el efecto de esta declaración? Al menos, es interesante señalar que el presidente dijo claramente que esperaba que el GT de HTTPBIS reconsiderara su posición en relación con el HTTP sin encriptar como opción para ese protocolo.

Gestión de las claves DS por terceras partes

En un "bar BoF" (reunión paralela que no forma parte del encuentro oficial) organizado por Olafur Gudmundson (Cloudflare), se exploró una posible extensión del EPP (o una solución RESTful al estilo WEIRD) para proveedores externos de DNS. Los participantes, todos a favor de la opción de administración de las claves por parte de terceros, provenían de registros (Afilias, VeriSign) y proveedores de servicios (Cloudflare, Akamai, Nominum).

Para brindar DNSSEC, quieren poder manejar los registros de DS de sus clientes, en lugar de tener que pasar por los registradores acreditados de la ICANN, que constituyen el primer paso que debe dar el usuario final para

firmar un dominio. Si bien se reconoció que algunos registradores podrían ver esta iniciativa como una manera de eludirlos (y sacarles parte del negocio), también se expresó cierta expectativa de que algunos de ellos podrían no estar interesados en gestionar la protección de DNSSEC para sus clientes, ya que esta tarea incluye mantenerse al día con las renovaciones de las claves. Se reconoció brevemente el problema de la asistencia al cliente en el caso de la existencia de fallas, y de la responsabilidad respecto de estas.

La principal vía técnica que se debatió fue una extensión del EPP que se describiría y discutiría en el GT de DNSOP (no en el GT sobre la extensión del EPP, que mantuvo una ardua discusión). Los proveedores externos recomendaron que la solución técnica fuera simple (algunos sostuvieron que la implementación completa del EPP era una carga innecesaria, y que preferirían presentar solamente una "muestra" al Registro para legitimarlos como administradores de DNSSEC para el cliente). A ICANN se le entregaría una solución técnica cuando estuviera lista. El paso siguiente será preparar un documento preliminar. Puede encontrarse una lista de correos que no es del GT aquí.

La respuesta de China a NetMundial

Dos congresos vinculados con Internet que se realizaron en China y Hong Kong desencadenaron debates paralelos acerca de un posible intento de China de "apropiarse" de un servidor raíz. El primer evento fue una reunión política de alto nivel que tuvo lugar en Wuzhen, China, del 19 al 21 de noviembre. El "Congreso mundial de Internet" (Cumbre de Wuzhen) fue organizado por la Administración del Ciberespacio de China, de reciente creación, y el Gobierno Popular de Zhejiang. Participaron funcionarios chinos y representantes de grandes empresas, como Tencent y Alibaba. El director general de ICANN, Fadi Chehade, fue criticado por su participación.

El título del encuentro, los temas tratados ("desafíos inéditos del desarrollo desequilibrado, crecientes amenazas a la ciber-seguridad, distribución despareja de recursos críticos de Internet") y sus objetivos declarados, entre ellos, "promover el desarrollo de Internet para que sea un recurso global compartido para la solidaridad y el progreso económico humanos" y "abrir nuevos capítulos en el desarrollo de Internet", explican, al menos en parte, el malestar expresado en países occidentales. Los títulos de los talleres incluyeron "Seguridad y cooperación en el ciberespacio", "Contrarrestar el ciber-terrorismo con una mayor cooperación internacional" y "La reforma a futuro: construir un ecosistema mundial de gobernanza de Internet".

Las dudas acerca del encuentro se reflejaron indirectamente en la ausencia de algunos oradores. (Para el diálogo de alto nivel sobre "un mundo interconectado compartido y gobernado por todos", los desertores incluyeron: Lu Wei, Ministro de la Administración del Ciberespacio de China, Kevin Rudd, ex Primer Ministro de Australia, Sato'Sri Ahmad Shabery Cheek, Ministro de Comunicación y Multimedios de Malasia y Daniel Sepulveda, Vice-Subsecretario de Estado de EE UU.)

También se organizó un diálogo de alto nivel sobre "un mundo interconectado compartido y gobernado por todos", un diálogo entre celebridades y una sesión solo para invitados sobre la "construcción de un ciberespacio pacífico, seguro, abierto y cooperativo". El programa podría interpretarse como una continuación en China de los eventos organizados por la UIT, una versión china del IGF o, incluso, la respuesta china a NetMundial.

Los anfitriones prepararon una "Declaración de Wuzhen", pero esta no fue publicada. Según el observador Izumi Aizu, un funcionario chino le dijo a un funcionario estadounidense que los anfitriones no presionarían para

llamarla declaración porque EE UU no había estado de acuerdo. Los organizadores del encuentro mencionaron en el programa que quieren que la Cumbre de Wuzhen se realice con regularidad.

No siete, sino millones de servidores raíz adicionales

El segundo evento fue un taller mucho más pequeño, organizado por ZDNS/BII y el Chinese Network Information Center (CNNIC), que trató el tema de la "disponibilidad de zonas raíz". Continuando con las presentaciones sobre la expansión de la zona raíz en la reunión del Grupo de Trabajo sobre el DNS en Londres, el taller, presidido por Warren Kumari (Google) y Paul Vixie (ex Director General de BIND), está analizando dos documentos preliminares. Una de las propuestas es la que presentaron Kumari y Paul Hoffman sobre la reducción de la latencia para pedidos de zonas raíz mediante una versión local del archivo de la zona raíz http://tools.ietf.org/html/draft-wkumari-dnsop-root-loopback-00 almacenada en la memoria caché. Fue presentada en Honolulu en la sesión de DNSOP, y fue muy bien recibida esta vez porque se agregó un nuevo elemento: impedir que el tráfico malicioso ascienda hacia la raíz. En la sesión de DNSOP, se pidió que los argumentos fueran respaldados con cifras en relación con los tiempos de conexión con servidores raíz "locales" (anycast).

La segunda propuesta es de Paul Vixie, Xiaodong Lee y Ziwei Yan, y el tema es "Cómo escalar el sistema de servidores raíz del DNS". Según el programa, el taller explorará las diferencias y similitudes entre las dos propuestas "con la idea de revisar ambos documentos".

Entretanto, en un post en su blog, Vixie pidió disculpas por haber sugerido agregar alrededor de siete servidores raíz en su primera propuesta, ya que se opone "sin ambages al agregado de más servidores raíz tradicionales". En cambio, la proposición modificada se basaría en el concepto de AS112 y permitiría que todos manejaran su propio servidor raíz, ya sea localmente o mediante el equivalente de anycast AS112 para la zona raíz de DNS. Vixie escribió:

"El problema con el actual sistema de servidores raíz no es que haya doce operadores de servidores, sino que no haya millones de operadores de servidores. Estoy trabajando para lograr que Internet tenga millones de servidores raíz y millones de operadores de servidores, y no un cambio insignificante de trece a veinte".

La IANA tendría que realizar ajustes menores:

- reservar dos bloques de Ipv4 e Ipv6 para propagar una versión adicional de la zona raíz;
- crear una copia, por lo demás idéntica, de la zona raíz del DNS con distintos registros de NS apex, pero firmados con la misma clave de zona raíz;
- crear algunos nombres de servidores (X.ROOT.IANA.NET y Y.ROOT.IANA.NET, por ejemplo), cada uno con una dirección en un prefijo IPv4 y otra en un prefijo IPv6;
- operar servidores de publicación capaces de servir a millones de servidores raíz "secundarios silenciosos";
- operar un servicio de suscripciones mediante el cual estos servidores puedan pedir y recibir notificaciones (NOTIFY) respecto de cambios en la zona raíz.

Grupos de Trabajo, BoFs (grupos informales de discusión)

Extensiones del EPP: si estandarizan las extensiones, ¡por favor estandaricen la mía!

El GT sobre extensiones del EPP sostuvo un debate interesante sobre si presentar la extensión propuesta como documento en el track estándar, en lugar de trabajar solamente con documentos informacionales o presentaciones individuales. La discusión también ayudó a aclarar la relación delicada entre los estándares del IETF y los arreglos contractuales de ICANN.

El presidente del GT, Jim Galvin (Afilias), resumió la discusión diciendo que, originalmente, el GT había pensado hacer que el documento "Extensión del registro para el EPP" fuera un documento en vías de convertirse en estándar, mientras que los documentos sobre extensiones individuales estaban abiertos al debate. Cada uno podría ser un documento en vías de convertirse en estándar, un RFC informativo o una presentación individual. La diferencia es que los primeros dos requieren consenso en el GT (lo que hace que el documento resultante sea una recomendación a la comunidad operativa). Las presentaciones individuales, en cambio, son una expresión de las partes, que documentan sus prácticas.

Galvin reconoció que determinar el consenso respecto de las extensiones del EPP en el GT era complicado, debido a que solo unos pocos usuarios de las especificaciones asistieron a las reuniones del IETF – los registros de dominios –, mientras que la comunidad registradora no estuvo representada. No obstante, los directores de área señalaron que la falta de evaluación en el GT del IETF podía compensarse con una evaluación en la comunidad de ICANN. Los autores de los documentos preliminares deberían documentar dicha evaluación.

Esto lleva, ciertamente, a una pregunta fundamental: ¿los documentos elaborados y/o evaluados en otra organización pueden recibir el sello de la estandarización del IETF? Es cierto que otras comunidades han presentado su trabajo al IETF [véase, por ejemplo, OAuth (autorización abierta), o el coded de audio para WebRTC]. Según los directores del área y el miembro del IAB Andrew Sullivan, no hay gran diferencia entre un RFC normativo y uno informativo. El hecho de que se aprobara un RFC del IETF no impediría que alguien presentara una nueva propuesta (una nueva solución) para el mismo problema.

Por otro lado, Chris Wright, de AusRegistry, se opuso a que se elevara lo que había sido planificado como presentación individual o documento informativo a la categoría "en vías de convertirse en estándar". Como su empresa desarrolló sus propias soluciones para algunos de los problemas planteados en los documentos preliminares del GT de extensiones al EPP, le preocupa que la transformación de esos textos en documentos en vías de convertirse en norma pudiera resultar contraproducente para él y sus registradores, porque ICANN los obligaría a adoptar las soluciones estandarizadas por el IETF en los nuevos contratos.

Si hubiera sabido que las propuestas se convertirían en documentos normativos, se habría opuesto aún más desde el comienzo, afirmó Wright. No es justo utilizar un consenso alcanzado fuera de un GT del IETF. Las discusiones deben empezar de cero, y deben compararse distintas soluciones para elegir una. Su respuesta a la posibilidad de elevar la categoría de la fase de lanzamiento del mapeo de extensiones es que él haría el esfuerzo de lograr que su propia solución también fuera aprobada como documento normativo del IETF.

Hay dos documentos de trabajo activos:

1 Registro de la extensión del EPP, presentado por VeriSign. Este introduce un procedimiento para el registro y la administración de las extensiones del EPP, y especifica un formato para que un registro de la IANA registre estas extensiones. El documento, pensado como un documento en vías de convertirse en norma, solo será informativo porque no especifica un protocolo, y fue presentado al IESG para su publicación.

2. Mapeo de EPP para Fase de lanzamiento, presentado por VeriSign, Cloud y CentralNIC. Este documento propone una extensión para las necesidades especiales de un registro cuando este lanza un nuevo TLD. En realidad, el documento fue elaborado fuera del IETF hasta la versión número 12, y luego transformado en un documento de GT. Según el presidente del GT, en este momento es un documento en vías de convertirse en estándar.

Se trataron brevemente tres documentos:

3. TMCH-SMD (Trademark Clearinghouse Signed Mark Data), confirmado también por Galvin como posiblemente en vías de convertirse en estándar (con fase de lanzamiento) debido a la evaluación de ICANN.

4. Mapeo de extensiones para la provisión de Nombres de Dominio Internacionalizados para el EPP: este documento está vencido, pero podría entrar en el proceso para convertirse en estándar, según Galvin.

5. Mapeo de extensiones para el "relay" de claves para el EPP: permite la transferencia de claves del DNSSEC, y fue redactado por SIDN Labs. Scott Hollenbeck, de VeriSign, recomendó utilizar la opción de transferencia ("transfer") actual para esto.

Los nuevos documentos preliminares presentados fueron los siguientes:

6. Agrupamiento de nombres de dominio (chino simplificado, tradicional), propuesto por Ning Kong, de CNNIC, a quien le preguntaron en qué medida la extensión podría ser utilizada independientemente de la política local de CNNIC.

7. Extensión de los mensajes de Servicio EPP: según el autor, Alexander Mayrhofer (nic.at), esta extensión permite transmitir mensajes adicionales del registro al cliente, el registrador. Las situaciones enumeradas en el documento preliminar incluyen, por ejemplo, avisarle al registrador que se transfirieron otros objetos junto con un nombre de dominio, o enviar advertencias cuando existen facturas impagas. Como señaló un proveedor de servicios de back-end (para .at, .berlin, .brussels, .hamburg, .reise, .tirol, .versicherung, .vlaanderen, .voting, .wien), solo había considerado una presentación individual o un documento informativo.

De todos modos, el GT tendría que re-redactar su acta constitutiva para poder ocuparse de nuevas tareas, afirmó Galvin.

DNSOP: DNS sobre TCP, minimización de Qname, cookies

La cuestión más importante en la que está trabajando actualmente el GT de DNSOP es la elevación de categoría de TCP como protocolo de transporte para el DNS. El principal objetivo del documento preliminar presentado por John Dickinson (Sinodun Internet Technologies) fue "poner a TCP en un plano de igualdad con UDP" y "convertirlo en un protocolo de transporte de la misma categoría". Los motivos mencionados fueron la privacidad y la prevención de ataques distribuidos por denegación de servicio (DDoS por sus siglas en inglés) (véase dprive más arriba). Dickinson enumeró lo que debe hacerse para compensar la pérdida de velocidad cuando se utiliza TCP en lugar de UDP: reusar la conexión, canalización y "TCP rápido". La canalización permite enviar consultas sin esperar respuestas pendientes.

"TCP rápido"

El "TCP rápido", que por ahora solo está disponible en Linux, permite enviar datos en el paquete SYN protegidos por una cookie del servidor. La primera respuesta, entonces, puede enviarse antes de que se complete la negociación en tres pasos. Esto permite aumentar la velocidad. El TCP rápido exige el cambio en el código y en el núcleo. El documento avanzará como documento del grupo de trabajo, ya que hubo considerable interés. Se mencionó como posible dificultad el hecho de que los servidores pueden elegir lo que aceptan de distintas maneras.

Lorenzo Colitti, de Google, dijo que su empresa tuvo que dejar de canalizar por la alta tasa de fracasos y, por ello, el lenguaje utilizado en el documento para establecer lo que los servidores deberían esperar y aceptar en consultas canalizadas tiene que ser más estricto. Colitti recomendó utilizar "DEBE", y su recomendación fue apoyada por Olafur Gudmundsson (Cloudflare). Sin este lenguaje imperativo, los servidores deberían indicar si admiten la canalización y la "apertura rápida".

Una de las cuestiones que se trató en relación con el debate TCP/UDP fue la necesidad potencial de una negociación previa acerca de cuándo un servidor del DNS cerrará una conexión TCP. Un escenario posible de ataque que se planteó fue el hecho de que se puede abrir muchas conexiones de TCP una vez que la persona que hizo la consulta original se fue. Si bien se creó un parche de seguridad para resolver este problema, abordado originalmente por Paul Wouters con la opción EDNS0 (edns-tcp-keepalive), este afirmó que algunos habían manifestado que podía utilizarse la propuesta para manejar conexiones de TCP. Ray Bellis (Nominet), quien presentó un nuevo documento preliminar, quiere dar lugar a una solución de menos peso: hacer que los servidores envíen un único bit de "conexión cerrada". El debate continúa.

QNAME

Acerca de la minimización de QNAME, el autor del documento, Stephane Bortzmeyer, declaró que todavía era necesario comprobar que el código funciona antes de llegar al último llamado. Bortzmeyer afirmó que estaría dispuesto a probarlo, pero no a hacer los cambios necesarios en Bind. No está convencido de que sea necesario un mayor análisis teórico. Según el secretario del GT, Paul Hoffman, también falta todavía la evaluación por parte de una larga lista de gente.

Cookies del DNS, anclajes de confianza negativos del DNSSEC

Además de trabajar sobre TCP y QNAME, el GT analizó una larga lista de temas muy viejos, viejos y más nuevos. Uno de los documentos recurrentes fue el que se ocupa de las cookies del DNS (Donald Eastlake) cuyo objeto es detectar ataques por denegación común de servicio y amplificación, falsificación o envenenamiento de la caché por parte de atacantes fuera del camino de resolución. Los clientes que utilizan el sistema de cookies

incluirían una opción Cookie de DNS en cada pedido de DNS. Según si una cookie del servidor ya fue guardada o no en la memoria caché, los clientes tienen que utilizar distintas variantes de la Cookie OPT. Nadie se opuso a la adopción del documento, que se remonta a 2006.

Los participantes en el GT estaban divididos respecto de la introducción de anclajes de confianza negativos. La idea, presentada por Jason Livingood (Comcast), es prevenir las fallas de dominios cuando estas resultan de errores de configuración del DNSSEC. La razón de la falla debe ser verificada por expertos en DNSSEC de un resolvedor recursivo/proveedor. Solo cuando se establece que la razón fue un error de configuración (y no conducta maliciosa), se debería configurar el anclaje de confianza negativo, instruyendo al resolvedor recursivo que no realice la validación DNSSEC para el dominio respectivo. Los usuarios pueden acceder al sitio correspondiente. Surgió la inquietud de que esto podría llevar a la existencia permanente de errores de configuración.

BoF sobre DBOUND: Se espera la creación de un nuevo GT sobre las maneras de indicar divisiones entre dominios públicos y privados o afirmaciones más amplias sobre políticas

DBOUND, "Límites entre dominios", se reunió informalmente en un "bar BoF" de aproximadamente 30 participantes para analizar la creación de un grupo de trabajo que elabore una alternativa a la Lista de Sufijos Públicos (PSL por sus siglas en inglés). La PSL, operada actualmente por Mozilla, tiene defectos conocidos (por ejemplo, actualizaciones lentas), y se ha dicho que, como herramienta, no responde satisfactoriamente al rápido crecimiento del nuevo espacio TLD. Después de que Andrew Sullivan (Dyn) elaboró el primer memo, "Establecimiento de los límites administrativos del DNS dentro de la zona del DNS", en marzo, Casey Deccio, de VeriSign, y John Levine impulsaron la elaboración del planteamiento del problema y del acta constitutiva de un nuevo GT. Según la presentación de Deccio al BoF, los puntos a tratar son evaluación de la eficacia, mantenimiento y distribución de la PSL, determinación de la "demanda de una identificación de la relación de dominio además de la provista por la PSL" y, finalmente, soluciones para mejorar y, también, ampliar la PSL. Los casos de uso que forman parte del documento actualizado de Sullivan incluyen:

- administración de estado HTTP mediante cookies (y otros usos de las cookies);
- indicadores de la interfaz de usuario;
- configuración de la propiedad document.dom ("podría contribuirse a la política del "mismo origen" de DOM mediante la posibilidad de identificar un ámbito común de políticas");
- mecanismos de autenticación del correo electrónico (incluyendo el DMARC, que recién se puso en marcha en el IETF);
- certificados de SSL y TLS;
- HSTS;
- Public Key Pinning;
- conectar dominios con fines de reportes/estadísticos.

La lista puede crecer, lo cual podría dificultar la identificación de una única solución. Según las discusiones que se están llevando a cabo en la lista de correos, existen actualmente alternativas a la PSL. Además de listas similares en la IANA y los operadores de registros, se hizo referencia a la llamada reconstrucción de "Bailiwick", que "aproxima la localización de un RRSET dentro de la jerarquía del DNS", descrita en una presentación del ISC sobre DNS pasivos del ISC.

DANE: Implementación y problemas de derechos de propiedad intelectual

Su implementación y una disputa sobre un anuncio acerca de derechos de propiedad intelectual realizado por VeriSign fueron los dos temas principales que se abordaron en el GT sobre DANE. El GT está trabajando sin grandes dificultades, y se espera que termine de tratar todos los temas que figuran en su Acta Constitutiva para noviembre del año próximo. Cómo promover la implementación es un tema de gran interés para el GT.

Según el co-presidente del GT, Warren Kumari:

Los documentos sobre SMTP y SRV están en la etapa de último llamado, o casi. Se espera que el próximo sea sobre claves crudas ("raw"). El documento sobre claves OpenPGP estará en la etapa de último llamado a principios del año próximo.

Modelo de seguridad de DANE

DANE IPSEC (seguridad del protocolo de Internet) (Paul Wouters dijo que LibreSwan está trabajando en este tema);

Enlace invertido servidor a cliente;

DANE 6698 y SRV se convirtieron en Estándar de Internet.

(Para los últimos cuatro, los presidentes del GT están buscando editores. Todos los documentos se encuentran aquí.)

A pesar de que DANE avanza más rápidamente que muchos otros GTs, existen algunos problemas de tiempos. Según Jacob Schlyter, de Kirei, los autores del documento sobre SMIME esperarían el resultado de la implementación por parte de VeriSign. Posiblemente, pasar los documentos sobre especificaciones básicas y SRV al trayecto hacia su conversión en estándar a fin del año próximo sea demasiado pronto, dado que DNSSEC, que era una condición para DANE, sigue esperando mayor despliegue.

VeriSign Labs desarrolló una implementación de DANE para Thunderbird (más sobre VeriSign Labs y DANE aquí), y abrirá el acceso al código resultante a todo el mundo. El firmado y el cifrado están separados: los usuarios tienen que invocar las acciones "Firmar DANE" y "Encriptar DANE" (¡hacer click!). Uno de los aspectos interesantes es que el texto sin encriptar no se guardará en ningún lado (el cifrado se realiza solamente cuando se muestra el texto en la pantalla). Uno de los temas debatidos fue que no se utiliza la función SMIME de Thunderbird ya existente. Eric Osterweil, de VeriSign Labs, que presentó la prueba, dijo que era mucho más fácil y rápido poner DANE al lado en vez de modificar el SMIME de Thunderbird. La prueba también brindará información para el documento sobre SMIME, dijo Schlyter. Se están realizando más pruebas aquí (Enigmail).

Si bien VeriSign Labs fue aplaudido por su trabajo de implementación, la empresa fue criticada por la notificación de derechos de propiedad intelectual que presentó al IETF. Su reclamo se basa en una solicitud presentada en noviembre de 2013 a la Oficina de Patentes de los EE UU, que tenía una lista de 20 reclamos. Las dos principales reivindicaciones son:

> *Lo que se reivindica:*
>
> *1. Un método de realizar operaciones en el sistema de nombres de dominio que comprende:*
>
> *acceso a un conjunto de políticas para la operación de un sistema de nombres de dominio (DNS) utilizando un sistema de nombres de dominio con extensiones de seguridad (DNSSEC);*
>
> *generación de un conjunto de respuestas a preguntas vinculadas con un conjunto de nombres de dominio de una zona, sobre la base del conjunto de políticas;*
>
> *generación de un conjunto de respuestas firmadas a partir del conjunto de respuestas y un conjunto de datos clave;*
>
> *almacenamiento del conjunto de respuestas firmadas en un archivo de zona;*
>
> *recibir una pregunta de un resolvedor y*
>
> *recoger una respuesta firmada basada en la pregunta recibida del resolvedor y el conjunto de políticas a transmitir al resolvedor.*
>
> *(….)*
>
> *11. Un sistema que comprende:*
>
> *una interfaz de red a un resolvedor que transmite una pregunta relacionada con un conjunto de nombres de dominio para una zona, con la existencia de un nombre de dominio que opera dentro de un sistema de nombres de dominio con extensiones de seguridad (DNSSEC) y*
>
> *un procesador que se comunica con el resolvedor a través de la interfaz de red y está configurado para acceder a un conjunto de políticas para la operación del sistema de nombres de dominio (DNS), generar un conjunto de respuestas vinculadas con un conjunto de zonas de un nombre de dominio basadas en el conjunto de políticas, generar un conjunto de respuestas firmadas del conjunto de preguntas y un conjunto de datos clave, almacenar el conjunto de respuestas firmadas en un archivo de zona que recibe la pregunta del resolvedor y recoger una respuesta firmada basada en la pregunta y en el conjunto de políticas para transmitir al resolvedor.*

No queda claro qué cubriría la posible patente, una vez otorgada, especialmente cuando parece estar relacionada con casos de uso de la tecnología. Debido al reclamo, Paul Wouters pidió que se descartara el texto propuesto por VeriSign sobre casos de uso de empresas. En cambio, se debería elaborar un nuevo documento mientras el reclamo siga abierto. Las reacciones en el GT fueron de cuestionamiento del efecto que podría tener un reclamo de patentes para casos de uso. A la vez, algunos señalaron que el estado de la técnica podría hacer que fuera fácil oponerse a una patente.

Según la presentación de casos de uso de VeriSign, las empresas quieren poder asociar claves con funciones (en lugar de nombres propios), comunicarse a través de los dominios y aprovechar sistemas de administración de identidades ya existentes.

Se debatió la implementación de DANE en general a partir de una presentación de Dan York ("La mayor parte de la gente no conoce la existencia de DANE"), quien enumeró preguntas para responder. Mientras que en algunos países (Alemania) hay medidas positivas hacia la implementación y un gobierno, el de Nueva Zelandia, decidió adoptar DANE (según Sebastian Castro, Internet.NZ), en otros países el desarrollo es lento pese al potencial percibido. Se hicieron propuestas durante la sesión: más publicidad para DANE, un manual adicional que sea fácil de leer, además del documento de instrucciones (Livingood, de Comcast) y hablar para lograr que se impulse su adopción (siguiendo a Internet.NZ). Pueden ver el apoyo que tienen DANE y DNSSEC aquí.

Área de seguridad

Dos presentaciones en el área de seguridad desencadenaron discusiones altamente políticas, que podrían haber constituido un debate plenario interesante. Los representantes de la ONG Article 19 promovieron que se revisaran los RFCs del IETF en relación con cuestiones de derechos. Si bien la privacidad es un aspecto obvio y bien cubierto que se controla cuidadosamente cuando se aprueban los RFCs, Niels ten Oever, Director del Área Digital de Article 19 y Joana Varon, de FreePress sostuvieron que los derechos humanos no se limitan a la privacidad. Sobre la base de una propuesta para investigar el impacto de los diseños de protocolos en los derechos humanos presentada por el experto en gobernanza de Internet Avri Doria, el grupo quiere revisar los RFCs existentes para ver qué derechos encarnan implícitamente. Según su entender, el RFC 1958 respalda el derecho al acceso a la información, los RFC 2369 y 2919, sobre aspectos de las listas de correos, equivalen a un derecho digital a la asociación, y los nombres de dominio que no son en inglés, normados en los RFCs 5890 a 5892, garantizan la diversidad cultural y los derechos de acceso.

La idea es establecer un grupo de investigación en el IRTF para avanzar con esta tarea. También quieren entrevistar a los autores para entender las motivaciones de la inclusión implícita de derechos en los protocolos. Si bien los participantes en la reunión del área de seguridad escucharon cortésmente, hubo algo de oposición contra "interpretar cosas que no están en los documentos" (Richard Barnes, de Mozilla). John Hall, director de tecnología del Center for Democracy and Technology, también recibió algunas críticas por su documento preliminar sobre tecnología de la censura. Si bien Hall dijo que esperaba que este fuera un documento de referencia para programadores que les permitiera tomar decisiones informadas cuando eligen sus estándares, los participantes en el IETF dijeron que podía muy bien servir como un instructivo para los propios censores.

En general, en esta reunión se debatió una cantidad sorprendente de temas vinculados con políticas. Aunque los participantes obligaron a los "muchachos de las políticas" a retroceder (con una cortesía sin precedentes, habría que agregar), la política ha llegado claramente al IETF. Mark Nottingham, presidente de HTTPBIS, publicó su propio documento preliminar sobre cómo manejarse con "las partes interesadas" en el mundo de la estandarización técnica, hasta ahora reservado a los especialistas, y, además, reconoció claramente (como lo hicieron otros participantes en el foro) que dicha estandarización es política.

"Cada vez que se toma una decisión, se realiza una declaración política, y tenemos que recordarlo", dijo Nottingham, agregando que el entorno idílico esterilizado de la informática que no necesita tratar con el desorden del mundo real era una falacia. Cuando esta autora le preguntó la diferencia entre el enfoque de su "Documento preliminar sobre actores" y el hecho de que las ONGs trajeran sus pedidos al IETF en persona, Nottingham respondió que su documento argumentaba en favor de considerar los intereses de los actores en el proceso de estandarización tal como son interpretados por los ingenieros.

La próxima reunión del IETF se realizará en Dallas del 22 al 27 de marzo de 2015.