INFORME IETF 90

Toronto

21-15 julio 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: http://www.centr.org/CENTR-Report-IETF890

LACTLD
Latin American and Caribbean ccTLDs Organization

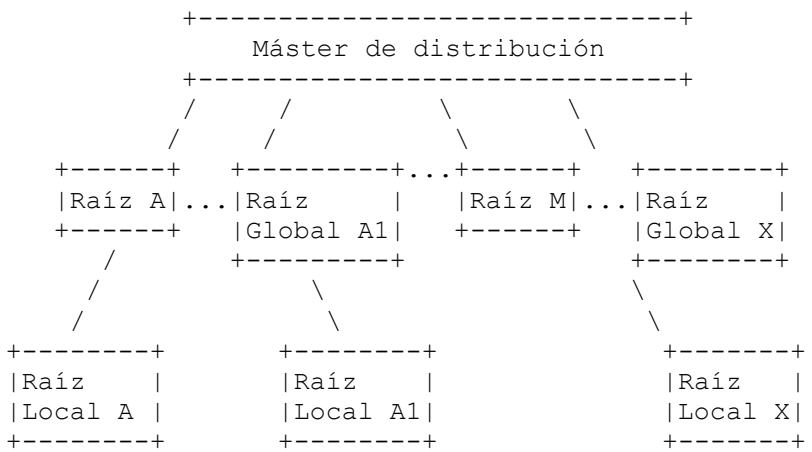
Destacados

Operaciones del Sistema de Nombres de Dominio (DNSOP por sus siglas en inglés): ¿“Ajustar la raíz” o cambiar la arquitectura del sistema de servidores raíz?

El grupo de trabajo sobre DNSOP no parece poder superar las nuevas discusiones políticas. Después de organizar un debate sumamente delicado en el último IETF sobre la posibilidad de que los órganos que establecen estándares asignen TLDs especiales (en paralelo al proceso de nuevos TLDs que está desarrollándose en ICANN), analizó en Toronto posibles cambios al núcleo del sistema de servidores raíz. Una propuesta de dos autores de CNNIC, Lee Xiaodong y Yan Zhiwei, y del fundador de BIND, Paul Vixie, desencadenó un intercambio breve pero agitado sobre la posibilidad de agregar nuevos servidores. Es interesante acotar que Xiaodong Lee también es miembro del Grupo de Coordinación de la Transición de la Administración de IANA (ICG por sus siglas en inglés).

La propuesta, titulada "Ajustar la raíz", afirma que es muy fácil agregar hasta siete servidores raíz a los 13 existentes sin que sea necesario recurrir al EDNS0 (Mecanismo de Extensión para el Sistema de Nombres de Dominio) o al TCP (Protocolo de Control de Transmisión) de apoyo (se ha puesto en duda que esto sea correcto). En todo caso, la idea de mantener los 13 servidores en el paquete de inicialización de 512 bits tuvo que ser abandonada con la llegada de las direcciones de IPv6, que son más largas. El límite de 512 bits había sido el argumento en contra del agregado de servidores raíz durante años.

Se presentaron dos modelos como alternativas posibles, que dejarían intacto el actual Sistema de Servidores Raíz: la IANA debería crear una copia firmada de la zona raíz y permitir que la propagaran nuevas partes (se podría acceder a esta copia a través de un nuevo conjunto de direcciones de IP bajo IN NS anycast-X1.iana-servers.net), o el nuevo proveedor debería establecer un contrato con cualquiera de los 13 operadores de servidores raíz. Ese servidor raíz podría estar “conectado globalmente mediante la técnica de anycast o implementado localmente y administrado y controlado de manera total por un CDO [País, Distrito, Organización]".



Según los autores, el segundo modelo sería retrocompatible. En respuesta a algunas preguntas realizadas por correo electrónico, Vixie comparó el modelo de contrato de RSO con una versión del anycast jerárquico de Joe Abley.

¿Por qué no darse por satisfechos con el anycast actual cuando la zona raíz ya es atendida en alrededor de 380 sitios en todo el mundo, según el documento preliminar (y existe una opción de agregar servidores con anycast en aquellos lugares que sientan la necesidad de tenerlo)? Los argumentos que se presentan en el documento preliminar son los siguientes: mejor distribución geográfica y control local para evitar el estancamiento que sigue a la falla de un servidor padre. El método anycast, además, no es "lo suficientemente abierto para satisfacer los requisitos especiales de un país, distrito u organización (CDO)". Al mismo tiempo, los expertos están de acuerdo en que las firmas de DNSSEC (extensiones de seguridad para el sistema de nombres de dominio) impedirían cambios en los datos originales de la zona.

Las reacciones al documento fueron variadas, pero la mayoría de los participantes en el GT cuestionan la necesidad técnica de agregar servidores raíz, incluso si pudiera hacerse. Según ellos, las cuestiones de la distribución geográfica y las respuestas para consultas locales ya han sido contempladas. La zona raíz ya no es un sistema jerárquico simple, si bien, por ahora, no es una red de seguridad completa. Por ello, desde el punto de vista de la mayoría, las razones de la expansión son puramente políticas (para algunos, solamente una cuestión de "orgullo nacional" chino).

Se considera que la elección de los lugares en los que se debería agregar servidores raíz lleva a un debate politizado. En conversaciones privadas, algunos argumentaron que, en lugar de incorporar nuevos servidores raíz, sería mejor reubicar los existentes (y un participante comentó que un país como China podría, ciertamente, pensar simplemente en "comprar" uno de estos servidores). Al contestar una pregunta sobre si China quería albergar uno o más x-rootservers Yan dijo que el primer objetivo era lograr un sistema mejor distribuido.

A pesar de las muchas objeciones presentadas al documento, hubo al menos algunas personas que se manifestaron en contra de ignorar problemas potenciales. El ex-presidente de DNSEXT, Andrew Sullivan, actual director de arquitectura de Dyn, dijo que el IETF no debería ocuparse solo de las preguntas fáciles y evitar las difíciles.

Más ideas de "ajustes"

Paul Hofman presentó otra idea para la distribución adicional de la información de la zona raíz. Según Hofman, mientras que Yan, Lee y Vixie se ocupan de los servidores de autoridad, su propuesta apunta a los resolvedores recursivos. Si el DNSSEC está instalado, el archivo de la zona raíz puede copiarse a cualquier resolvedor recursivo que puede, a su vez, ayudar a aliviar la carga de los servidores del DNS. Hubo bastante oposición a esta propuesta. Los participantes hicieron la misma pregunta que había surgido respecto de la solución del servidor de autoridad: ¿de qué problema se ocupa? Con actualizaciones del archivo de zona de los servidores raíz que se realizan cada hora, los resolvedores podrían consultar directamente a los servidores raíz con pedidos de actualizaciones.

La tercera presentación fue mejor recibida. Nuevamente, se trató de un documento elaborado por autores de CNNIC, incluyendo a Ning Kong. Este documento se ocupa en más detalle del problema general de cómo ubicar mejor los servidores del DNS en términos de geografía y topología. Ning Kong propone un algoritmo para calcular dónde colocar los servidores, dependiendo de los factores que se deseen optimizar (velocidad, presupuesto u otros).

La fórmula presentada en el documento podría adecuarse a los nuevos gTLDs para lanzar al mercado sus nuevos TLDs. Si bien algunos aplaudieron este texto como positivo para su trabajo (Lars Liman, de Netnod, quien es, además, miembro del ICG), otros opinaron que era "demasiado parecido a una investigación" para incorporarlo al proceso del GT. Por otra parte, la propuesta podría discutirse en mayor profundidad en la reunión del Centro de Operaciones, Análisis e Investigación (OARC por sus siglas en inglés) el próximo otoño.

Cuestiones no técnicas a discutir en el GT

Queda por verse cómo seguirán debatiéndose los temas de ajuste. Dado que el IETF también está pasando por la transición de la IANA, podría pensarse que iniciar el debate sobre el tema, sumamente delicado, del sistema de servidores raíz sería poco oportuno. También se agrega a la lista de cuestiones políticas recogidas recientemente por el GT de DNSOP.

Respecto a los nombres especiales (los TLDs que el IETF delegará por fuera del proceso de ICANN), que se trataron durante el IETF 89, no se produjeron novedades. Sin embargo, la co-presidente Suzanne Woolf mencionó que el Acta Constitutiva recién actualizada permitiría ocuparse del tema de la delegación de los dominios especiales y/o de la posible actualización de la RFC (solicitud de comentarios) que rige ese proceso. Recientemente, se enviaron dos solicitudes al IETF con pedidos de TLDs de uso especial (una de ingenieros que trabajan en TOR, la otra del grupo que se ocupa de las colisiones entre nombres).

El tercer tema que es también bastante político es el de los documentos preliminares que quieren aumentar la privacidad en el DNS. Según el co-presidente del DNSOP Tim Wicinski (Salesforce.com), esta cuestión sigue estando "muy presente en las mentes de todos", pero no se destinó ningún espacio para tratar el progreso de los documentos ni para realizar comentarios adicionales sobre el tema (véase, por ejemplo, el posteo de Vixie).

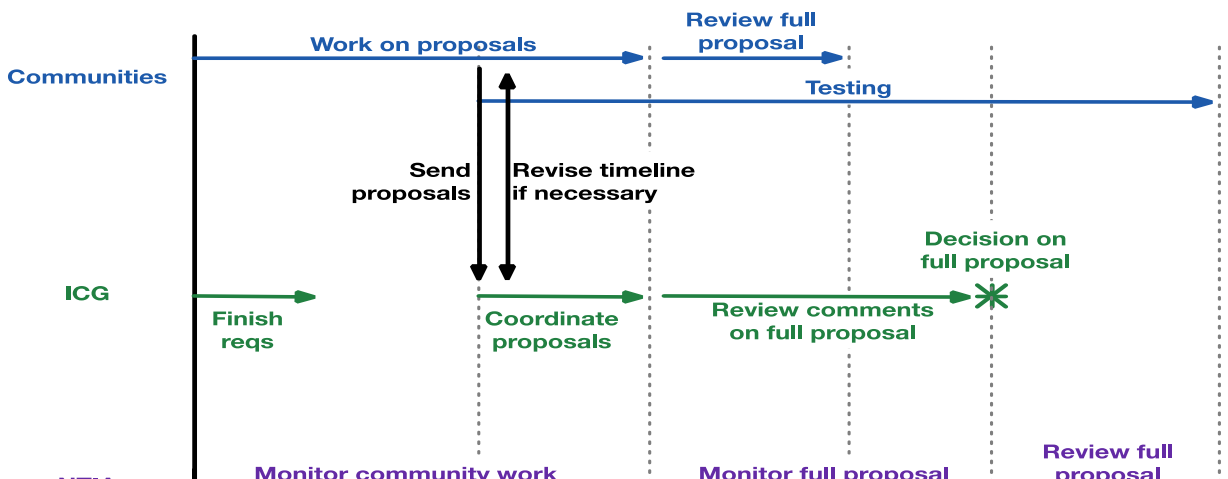
Además de las cuestiones "operativas" clásicas del DNSOP, la nueva Acta Constitutiva contempla el trabajo con protocolos, de algún modo, retomando aspectos que habían quedado pendientes en el GT de DNSEXT. Si el GT trata todos los temas más políticos, a sus miembros les espera una época interesante.

Un grupo de trabajo para el plan de la IANA: un espacio para el consenso

De los distintos clientes de la IANA, el IETF tuvo la primera oportunidad de reflexionar sobre el primer encuentro del ICG, que se realizó los días 17 y 18 de julio. Este grupo, de 30 miembros, trabajó en un Acta Constitutiva que enumera cuatro tareas para realizar hasta el 15 de septiembre de 2015:

- establecer un enlace entre todas las partes interesadas, incluyendo las comunidades operativas, con el objeto de recoger propuestas de órganos operativos y de la comunidad más amplia;
- evaluar propuestas de las comunidades operativas en cuanto a la compatibilidad y la interoperabilidad;
- elaborar una propuesta completa;
- socializar la información sobre este proceso.

La reunión del BoF (grupo informal de discusión) sobre el IANAplan en Toronto creó un grupo de trabajo del IETF cuya función no se delineó claramente en la primera reunión. Si bien se lo describió como un espacio de consenso necesario en relación con la presentación del IETF al ICG, existió acuerdo de que el trabajo propiamente dicho debía llevarse a cabo en el Consejo de Arquitectura de Internet (IAB por sus siglas en inglés) debido al ambicioso cronograma presentado por Alissa Cooper, del IAB (y miembro del ICG):



En total, la comunidad del IETF tiene cuatro representantes (sin contar los de ISOC u otras comunidades técnicas afines como, por ejemplo, el Comité Asesor sobre Servidores Raíz, RSSAC por sus siglas en inglés): el presidente del IETF, Jari Arkko, la miembro del IESG Alissa Cooper, el presidente del IAB, Russ Housley, y Lynn St. Amour. No obstante, Arkko (delegado del IETF en el ICG junto con Alissa Cooper) explicó por qué era necesario tener una mayor participación de la comunidad del IETF. La presentación de una propuesta final por parte del Foro acerca de la modalidad de gobierno de la IANA le daría mucho más peso a la postura de esta organización.

¿Los procesos de gobernanza del IETF son muy sólidos o poco legítimos?

En esencia, el presidente del IETF y muchos otros impulsaron una lógica de "dejar las cosas como están" o "no cambiar nada". La propuesta presentada por Andrew Sullivan describió el posible aporte del IETF al proceso del ICG: un inventario de los acuerdos y procesos (incluyendo procesos de apelación) que están en vigor en el Foro. Varios participantes señalaron que los procesos del IETF vinculados con la IANA debían aparecer como "sumamente sólidos".

Lo que subyace a esta lógica no es necesariamente la satisfacción con el modelo actual ni la confianza en él. Más bien, algunos antiguos participantes en el IETF consideran que los intentos de hacer transformaciones importantes conllevan algunos peligros. Existe la posibilidad de que una discusión sobre el cambio pueda resultar en peleas políticas duras que consumirían mucho tiempo, llevando a la postergación de la partida de la Dirección Nacional de Telecomunicaciones e Información estadounidense (NTIA por sus siglas en inglés). Algunos dicen, incluso, que si esta no se logra durante el corriente periodo legislativo, podría haber un nuevo cambio de humor en la política estadounidense.

Además, como lo dijo un participante, si uno hurga lo suficiente, puede desenterrar hasta qué punto algunas de las estructuras que involucran al IETF son "artesanales" en algunos aspectos. Estos aspectos de un sistema que fue alguna vez bastante informal, y que ha crecido enormemente, pueden carecer de legitimidad si se miran desde fuera de la comunidad técnica, que está muy unida.

En contra de la visión de que no hace falta ningún cambio y de que, por ello, ICANN debería conservar la función de la IANA y cumplir, hubo al menos algunas advertencias severas de que, si bien el IETF puede no estar interesado en cambiar, otras comunidades pueden muy bien estarlo, y el Foro debería estar preparado para responder a esos pedidos de cambio. Arkko estuvo de acuerdo: manifestó que los integrantes del IAB que estaban involucrados en este proceso habían considerado alternativas y estaban siguiéndolo de cerca.

Puede esperarse que se considere un documento preliminar de la presentación del IETF durante la última reunión del Foro en 2014, ya que, fundamentalmente, ese documento informará acerca de la situación actual. En Toronto, el miembro del ICG Russ Mundey (representante de SSAC) manifestó su esperanza de que el IETF pudiera servir de modelo para los procesos de consulta con la comunidad, y pidió que esta institución enviara su presentación al ICG temprano. A la vez, el ICG ya ha heredado varios genes de las organizaciones técnicas: la adopción de una Carta Constitutiva, el uso del "consenso aproximado" como forma de alcanzar un compromiso en el grupo y la cooperación a distancia intensiva (véase la lista de

direcciones de alto volumen de tráfico).

Será interesante ver si el proceso, que está siendo claramente liderado por la comunidad técnica, es lo suficientemente rápido y fluido como para evitar posibles "ataques de canal lateral".

El IETF no aceptará más estándares de cifrado que vengan "en bandeja de plata"

El Grupo de Trabajo de Seguridad de la Capa de Transporte (GT de la TLS) decidió estandarizar las nuevas curvas elípticas para el uso en la TLS (preferiblemente, para que puedan usarse también para PKIX) y pidió al Crypto Forum Research Group que eligiera una o varias curvas. En la reunión del IETF en Toronto, la criptografía se convirtió repentinamente en un tema inusualmente candente. Varios participantes afirmaron que el Foro debería dejar de aceptar estándares en bandeja de plata, incluidos los que ellos mismos presentan.

Hasta ahora, el IETF ha dependido en gran medida de estándares de cifrado publicados por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST por sus siglas en inglés). Sin embargo, después de las revelaciones de Snowden sobre el programa de la Oficina Nacional de Seguridad de Estados Unidos (NSA por sus siglas en inglés) y sobre los bien planeados intentos de este organismo de debilitar los estándares de cifrado, especialmente a través de su relación especial con el NIST, existe considerable desconfianza hacia los estándares de este instituto. Luego de que este finalmente retiró su generador de números aleatorios de curva elíptica y empezó a revisar las posibles debilidades de su proceso de estandarización, se consideraron cambios a la "función de receptor de estándares de cifrado" del IETF.

El CFRG dio un primer paso al dedicar la mayor parte de su sesión en Toronto a escuchar presentaciones de expertos en cifrado, incluyendo a Dan Bernstein, investigador de la Universidad de Chicago que trabaja actualmente en la Universidad de Eindhoven, y a la experta alemana Tanja Lange (Universidad de Eindhoven), por una parte, y a Brian La Macchia, director de cifrado y seguridad de Microsoft, y Craig Costello, investigador de cifrado de Microsoft, por la otra. Los dos grupos presentaron sus propuestas de nuevas curvas elípticas. Lange brindó un panorama del cifrado de curvas elípticas que fue muy bien recibido.

Nuevas curvas posibles

En 2006, Bernstein ofreció la nueva curva 25519, que está siendo utilizada por TOR, Apple, IOS y otros. Ahora la propone como una opción para la TLS. El año pasado, Lange y Bernstein produjeron una nueva curva, la 41417, a partir de un pedido del fundador de PGP, Phil Zimmermann. El investigador de Microsoft, por su parte, propuso la curva NUMS (cuyo nombre corresponde a las siglas en inglés de "nada debajo de la manga").

Los dos grupos parecen favorecer el cambio de las funciones utilizadas para calcular las curvas. Mientras que hasta ahora la función Weierstrass había sido la preferida para las curvas del NIST, en Toronto se propusieron las funciones de Edward y una variación llamada "Edward retorcida", consideradas más rápidas y seguras.

Según un resumen del nuevo co-presidente del CFRG, Kenny Patterson, otros aspectos en los que está surgiendo consenso son:

- debe existir protección contra ataques de canal lateral;
- los elementos básicos de la selección de las curvas definidas sobre un campo primo; orden primo o casi primo; seguridad de giro;
- los algoritmos existentes deben tener el apoyo de ECDHE, EC, DSA y ECDH;
- la rigidez en la generación de curvas.

Paterson también presentó un cronograma para la tarea, alegando que esperaba alcanzar consenso respecto de los requisitos en solo dos semanas y, respecto de las curvas, en cuatro. A partir de allí, las recomendaciones finales para el GT sobre TLS llevarían otras dos semanas. Según el co-presidente Sean Turner, este GT espera recibir una recomendación para una o unas pocas curvas, y elegiría las que recomiende el CFRG.

Reacción del NIST

Obviamente, el NIST parece estar algo preocupado por la pérdida de su posición como productor más general de estándares de cifrado (no solo para los Estados Unidos). Tim Polk, funcionario de este instituto, que fue director del área de seguridad, anunció que el NIST también estaba considerando estandarizar nuevas curvas elípticas. En todo caso, no había estado a favor del grupo grande de curvas seleccionadas que están siendo estandarizadas ahora.

Polk se refirió a un informe reciente realizado por un grupo experto externo sobre las debilidades de los estándares individuales y el proceso de selección y estandarización del NIST en su totalidad. Ed Felten, miembro del grupo y profesor de la Universidad de Princeton, recomendó fuertemente que este instituto estandarice nuevas curvas elípticas. También insistió en que revise el Memorando de Acuerdo firmado con la NSA para recuperar y fortalecer la independencia del NIST en su tarea de provisión de estandarización de cifrados. Según Polk, este instituto está haciendo consultas acerca del informe final del grupo de expertos y, si las partes interesadas recomendaran agregar curvas nuevas, el organismo lo haría.

Paterson, el nuevo co-presidente del CFRG, interrumpió a Polk para recordarle que el espacio había sido reservado para debatir las curvas presentadas en Toronto. Por cierto, hay una competencia oculta para ser el proveedor de estándares de cifrado del IETF y, si bien los estándares federales de procesamiento de la información (FIPS por sus siglas en inglés) seguirán siendo obligatorios para los proveedores estadounidenses en muchas instancias, el IETF puede surgir como nuevo proveedor en otras. Para promover el desarrollo de estándares por parte del Foro, se eligieron dos nuevos co-presidentes para el CFRG: además del académico británico Paterson (Royal Holloway), Alexey Melnikov (Isode). Estos asumirán en lugar del co-presidente que queda, Kevin Igo (NSA), luego de su jubilación el año próximo.

Grupos de Trabajo

DANE (Autenticación de entidades con nombre basada en el DNS)

Se ha realizado un avance considerable en DANE, que puede muy bien llegar a convertirse en una aplicación excelente para el DNSSEC, como nos dijo el co-presidente de DANE, Olafur Gudmundsson. Este señaló particularmente la posibilidad de que las empresas utilicen DANE para un sistema unificado de claves en el futuro y, así, ahorrar dinero que se gasta ahora en certificados. Además, indicó la importancia del documento preliminar sobre claves "sin procesar" que se debatió durante el foro. Este aclarará que los dominios asegurados por DNSSEC puede convertirse en el lugar para almacenar material de claves de usuarios de correo electrónico. Hasta ahora, se considera que la especificación de DANE privilegia (o hasta obliga a utilizar) los certificados, incluso cuando no hay ningún proveedor de certificados involucrado.

El GT de DANE está por terminar los documentos sobre DANE-SMTP y DANE-SRV, e iniciará el proceso de publicación como RFCs. Ya se están informando implementaciones del correo electrónico protegido por DANE para una creciente lista de proveedores de correo electrónico en Alemania (véase la lista). No hay implementaciones para Postfix ni Exim Mail Software.

Otro documento preliminar que se espera que entre en el proceso de publicación es el que se ocupa del DANE/OpenPGP. Según su autor, Paul Wouters (Red Hat), solo falta realizar pequeñas correcciones. Este documento apunta a que el DNS protegido por DNSSEC se convierta en el espacio central donde obtener la clave pública para encriptar correos con PGP.

DANE OpenPGP y DANE SMIME, un tema que aún se está debatiendo en el GT, tenían que ver, más que nada, “con brindar un lugar estándar para controlar claves en un espacio seguro y autenticado: dentro del propio dominio controlado del usuario", explica Wouters. Las claves se guardarían en el DNS bajo un dominio especial, como por ejemplo XXXX._openpgpkey.mydomain.ca., donde XXXX sería el sha224 de la izquierda de la dirección electrónica. Ya existe una implementación que permite la obtención automática de la clave de PGP con MTA/MUA. Según Wouters, buscará registros de openpgpkey y, si los encuentra, encriptará el correo y reescribirá el asunto, cambiándolo por "[correo encriptado]".

Wouters también presentó el documento preliminar sobre claves sin procesar, escrito por John Gilmore, de Electronic Frontier Foundation. Este documento propone cambiar la RFC 6698 sobre DANE/TLSA en lo que se refiere a las claves públicas. 6698 especifica de manera explícita que los registros de TLSA solo pueden almacenar certificados de PKIX. Según Gilmore, como el GT de TLS había aprobado claves públicas sin procesar. (http://www.rfceditor.org/rfc/pdfrfc/rfc7250.txt.pdf), la especificación de DANE debería ser actualizada correspondientemente. Es la actualización de la clave pública sin procesar de TLS-DANE la que permitirá, finalmente, lo que Gudmunsson llama "generación de claves públicas unificadas". En lugar de utilizar certificados para TLS y claves para otras aplicaciones, todas las claves pueden almacenarse y obtenerse en el DNS. Gudmundsson calificó la tecnología de "disruptiva”.

Durante la sesión en Toronto, se consideró evaluar las cuestiones vinculadas con claves sin procesar como otro tema relacionado con la actualización del DANE. Luego de trabajar sobre el documento de pautas operativas, Viktor Dukhovni (también autor del DANE SMTP) propuso utilizar dicho documento como base para generar un DANEBIS.

A la vez, se analizó la posibilidad de utilizar más la generación de claves autenticadas por DNSSEC y almacenadas en el DNS para SIP (véase el GT sobre SIPCORE) y NAT-Traversal (GT sobre TRAM: TURN revisado y modernizado).

Httpbis – Debate sobre proxys

El GT sobre httpbis ha estado avanzando en su lista de temas para completar la actualización de http, mientras que la renovación de http 1.1 está por concluirse gracias a la aprobación de un conjunto de

documentos (RFC 7230, 7231, 7232, 7233, 7234 y 7235). Http 1.1 modularizó la especificación original, y se espera que esto facilite su actualización en el futuro. Según Julian Rescke, de Greenbytes, coautor de 1.1, http 2 solo ampliará 1.1 y cambiará algunas partes, es decir, el formato de la conexión.

Una de las dos sesiones sobre httpbis en Toronto se dedicó a debatir la posible estandarización de un proxy para interceptar, un tema que ya se había discutido. Las inquietudes que se expresaron incluyeron temas como el costo del tráfico encriptado de punta a punta para conexiones vía satélite en áreas remotas, especialmente en países en desarrollo con poco ancho de banda que necesitan bloquear el acceso y, a la vez, cumplir con las normas de los reguladores.

Dados los desarrollos actuales, afirmó Peter Lepeska, director general de “Acceleration research Technologies” de ViaSAT, con el uso obligatorio de TLS para http 2.0, la red podría estar usando https casi exclusivamente en los próximos años. Además, Lepeska advirtió acerca de los efectos negativos para la compresión, el caché y la aceleración, dando el ejemplo de Opera Mini (que desencripta en el nivel de servidor) como el sistema preferido en muchas áreas de África con poca amplitud de banda. Según su lógica, encriptar todo de punta a punta incrementaría la brecha digital. Tanto Lepeska como Salvatore Loreto, de Ericsson, urgieron al GT que definiera y estandarizara un "proxy intermediario" con el "consentimiento de los usuarios".

Adam Langley y casi todos los oradores en este debate advirtieron acerca de la posibilidad de permitir otra invasión del tráfico de punta a punta. A pesar de que el consenso fue casi unánime que los proxies para interceptar no deberían ser estandarizados para la siguiente generación de http y que se le pidió al director del área de seguridad, Stephen Farrell, que registrara dicho consenso, el presidente del GT, Mark Nottingham, no dio el tema por concluido. Nottingham, que está trabajando con Akamai, redactó un documento preliminar sobre el problema de los proxies (y los casos de uso legítimo e ilegítimo). Lo sintetizó en Toronto diciendo que dos de las opciones serían publicar el documento preliminar sobre el problema de los proxies o estandarizar proxy.pac (también hay un viejo documento preliminar del IETF) o, sino, pensar otras soluciones para otros casos de uso.

La situación con los proxies podría compararse con la del NAT (traductor de direcciones de la red). Este último no fue estandarizado porque el IETF consideró que no era la solución tecnológica apropiada. Después de su rechazo, el NAT fue ampliamente implementado sin estandarizar, lo cual hizo que fuera necesario encontrar una solución, por ejemplo, para el SIP. El trauma del NAT, como lo llamó un participante, puede ser la causa de la vacilación ante la necesidad de tomar una decisión definitiva sobre proxies.

Weirds

RDAP (Acceso y Preservación de Datos de Investigación) está cerca de completarse. Los presidentes del GT decidieron establecer un plazo de entrega en septiembre para todos los documentos de los grupos de trabajo, y poner una última fecha para el IETF en octubre. Respecto del documento sobre arranque que se discutió durante la reunión en Toronto, hubo pedidos de tratar dos temas. Uno de ellos está vinculado con consultas sobre internacionalización (a tratarse en un apéndice). El otro está relacionado con las tareas de IANA vinculadas con el establecimiento de nuevos registros para permitir encontrar servidores de RDAP (IPv4, IPv6, ASN y DNS). Peter Koch, de DENIC, cuestionó la oración que dice que "las políticas de registro para los nuevos registros quedarían a cargo de la IANA". Además, Andy Newton presentó una nueva propuesta sobre el uso de RDAP para políticas de enrutamiento que abriría otra ronda de discusiones.

Se plantearon preguntas acerca de la poca actividad en este GT (allí no pasa nada). El cronograma estricto, combinado con la amenaza de que el grupo se cerraría sin producir un documento, tiene por objeto llevar la tarea a su fin. En una conversación privada, Jim Gavin (Afilias) dijo que podía visualizar a ICANN dirigiendo la operación de los Registros de Dominio en cuanto se produjera una RFC. Scott

Hollenbeck (VeriSign) afirmó que desde el punto de vista de VeriSign, no tendría sentido introducir el whois amplio en paralelo a RDAP, pero ICANN seguía pidiendo la implementación de aquel.

Será interesante observar cómo funciona la introducción de RDAP una vez que llegue a ICANN, especialmente si tenemos en cuenta el informe recién terminado del Grupo de Trabajo Experto sobre Futuros Servicios de Directorio de los Registros (EWG por sus siglas en inglés). Según Hollenbeck, quien ha participado activamente en ambos espacios, el informe del EWG, que propone una base de datos centralizada y acceso a los datos de registro, fue coordinado en cierta medida con WEIRDS.

Novedades del IETF

El IETF está en proceso de actualizar sus sistemas. Eligió Cloudflare como proveedor de servicios de CDN (red de distribución de contenidos) y, además, está evaluando propuestas para una herramienta de programación de reuniones, un nuevo sitio Web, un servidor de IMAP (protocolo de acceso a mensajes de Internet) y un archivo de correos electrónicos.

Transparencia y buena conducta

Los telechats del IESG estarán abiertos a observadores hasta el IETF 91, como experimento para permitir a los autores y a otros que sean testigos de los intercambios. El mayor debate durante la plenaria administrativa tuvo que ver con la futura moderación de la lista de discusión del IETF, donde se han producido ataques personales. La moderación también se convirtió en un problema en el caso de otro experimento: una opción de etherpad para "ponerse en la fila" para utilizar el micrófono en la plenaria. Cuando los participantes empezaron a burlarse del pad, el presidente lo "censuró". Arkko también desafió a la comunidad del IETF a seguirle el ritmo a la tecnología. Las organizaciones que producen estándares tienen que trabajar rápido para continuar siendo relevantes.

Premio Postel

Este año se entregó el premio Jon Postel al Dr. Pun, fundador de la Red de Conexiones Inalámbricas de Nepal. Pun empezó a conectar aldeas remotas en el Himalaya a la red en 2006. Debido a restricciones a la importación de equipos de conexión inalámbrica, hubo que "contrabandear" repuestos a través de la frontera, y el Dr. Pun enseñó a los aldeanos y estudiantes a armar e instalar los equipos. Parece ser un bien merecido premio a un gran esfuerzo.

El IETF 91 se realizará en Honolulu, Hawaii, del 9 al 14 de noviembre.