INFORME IETF 89

Londres

3-7 marzo 2014

Monika Ermert
para

CENTR &
LACTLD

Edición en castellano revisada y actualizada por
Hugo Salgado (nic.cl)

LACTLD agradece la colaboración de CENTR por los aportes fundamentales para el financiamiento de la iniciativa, así como al apoyo de ISOC y la contribución de Hugo Salgado. Para acceder a la versión en inglés de este informe: https://centr.org/CENTR-Report-IETF89

LACTLD
Latin American and Caribbean ccTLDs Organization

INDICE

Destacados.....2
El GT sobre el DNS necesita más reuniones de trabajo 4
Nombres especiales: algo menos caros que 185.000 dólares.....7
Cerrar filas: Gobernanza de Internet@IETF 9
Grupos de Trabajo, BoFs 10
Novedades del IETF 14

Destacados

Mejorando defensas: seminario STRINT y más

Durante casi un año la comunidad técnica ha estado procesando el constante flujo de revelaciones sobre la vigilancia permanente de las comunicaciones en Internet, la cual ha llegado al punto de socavar e, incluso, manipular las tecnologías de seguridad. En todas sus declaraciones públicas sobre la reunión del IETF, su presidente, Jari Arkko, ha afirmado que la tarea de "reforzar la seguridad" había ocupado gran parte del tiempo de trabajo del Foro.

Según Arkko, dado que la comunidad del IETF se comprometió en la sesión plenaria técnica en Vancouver a empezar a mitigar el "ataque" de la "monitorización permanente" mediante el diseño de protocolos y a "hacer que la monitorización permanente sea significativamente más cara o imposible de implementar", es hora de que cumpla con su promesa. La aprobación del documento Buenas Prácticas Actuales, basado en ese compromiso [y enviado a la cola del editor de las solicitudes de comentarios (RFC por sus siglas en inglés) durante la reunión en Londres], fue, sin duda, solo el primer paso, declaró el presidente durante la plenaria administrativa en Londres. Diseñar e implementar cambios en los protocolos es más difícil y, seguramente, no tan fascinante.

Arkko mismo señaló el aumento de las conexiones seguras como un resultado más visible de estos esfuerzos. Una mirada a las reuniones del grupo de trabajo en Londres también muestra la gran cantidad de energía invertida en el trabajo en este tema. Además de una explosión del diálogo sobre la privacidad del DNS (véase más abajo), deben tenerse en cuenta el trabajo continuo en la renovación del http y las consideraciones acerca de cómo avanzar en la selección de los algoritmos de criptografía [véase el informe sobre el GT del SAAG (Grupo Asesor sobre el Área de Seguridad) más abajo].

El uso de la TLS en Aplicaciones

Se asignó un GT totalmente nuevo (que ni siquiera fue precedido por un BoF o grupo informal de discusión) para analizar "el uso de la TLS (seguridad de la capa de transporte) en aplicaciones" (UTA por sus siglas en inglés). Orit Levin, Gerente Principal de Programas de Microsoft y Profesional de Estándares, presentó los objetivos de un futuro GT sobre el UTA. En esa ocasión, afirmó que hasta el momento existe una falta de interoperabilidad y de implementación de la TLS para aplicaciones.

Los insumos a producir que se analizaron en la reunión sobre el UTA son: documentación de brechas de seguridad en los protocolos de aplicaciones, pautas para utilizar la TLS y un conjunto de documentos que describan las prácticas actuales y futuras para el uso de la TLS con protocolos de aplicaciones de SMTP, POP, IMAP, XMPP y HTTP 1.1. Además, el BoF intercambió ideas acerca de la elaboración de un documento sobre "encriptación oportunista", un tema candente en muchas discusiones.

Sesión de trabajo sobre "Fortalecimiento de Internet Contra la Vigilancia Permanente (STRINT por sus siglas en inglés)"

La encriptación oportunista también fue un tema que se discutió vivamente durante una sesión de trabajo sobre "Fortalecimiento de Internet contra la Vigilancia Permanente" (STRINT). Esta sesión fue organizada por

el Consejo de Arquitectura de Internet (IAB por sus siglas en inglés) y el W3C (Consorcio de la World Wide Web) y financiada, en parte, con fondos para la investigación de la UE, justo antes del encuentro del IETF.

Asistieron a la reunión más de cien expertos que analizaron casi setenta documentos, presentados por los participantes, sobre una serie de temas técnicos y de políticas vinculados con la vigilancia permanente.

El Director Adjunto de Seguridad del IETF, Stephen Farrell, resumió el consenso aproximado al que se llegó en la reunión acerca de la necesidad de explicar la encriptación oportunista en un RFC "al estilo de un libro de recetas". En la lista de tareas acordada por el grupo también se encuentra la elaboración de una guía que recomiende un mecanismo de seguridad/encriptación que esté "activa por defecto", y una nueva edición de (o agregado a) la Buena Práctica Actual BCP 72 en el apartado sobre seguridad de las RFCs.

Durante la reunión sobre STRINT hubo algunas voces prominentes – entre ellas, la de Phil Zimmermann, programador de PGP (Circle), y la de Steve Bellovin (Universidad de Columbia) – que enfatizaron la necesidad de avanzar más en relación con la encriptación. Esta es la mejor decisión, debido a los cambios producidos en el análisis de amenazas y el aumento de la potencia computacional.

En la sesión de discusión se definió la encriptación oportunista como encriptación sin autenticación previa mediante certificados, registros DANE o similares. Se presentó una implementación ilustrativa para MPLS (Comunicación Multiprotocolo Mediante Etiquetas). Según una clara mayoría de los participantes, una ventaja de utilizar la encriptación oportunista rápida como estándar "activo por defecto", sería que no haría falta que los usuarios entendieran, ni siquiera que se les preguntara si quieren utilizarla.

Por cierto, existe cierta preocupación de que la medida, que deja abierta la comunicación a los ataques activos (al tiempo que previene los ataques de tipo pasivo, de vigilancia), conduciría a una actitud de complacencia y, así, se retardaría el proceso de avance hacia la seguridad real de punta a punta. ,Un proyecto interesante que está en marcha, por ejemplo, es el Proyecto de Encriptación Abierta, que actualmente funciona con un diseño y prototipo(s) de un chip abierto de encriptación y una cadena de herramientas segura.

Se discutieron otras acciones posibles en la sesión de STRINT, entre ellas, un día mundial de certificados incorrectos (con representantes de Chrome, Mozilla, Apple y Microsoft en el mismo sitio). Se dedicó una ronda entera de conversaciones al problema de los meta-datos y su posible minimización. Aquí se apuntó a la comunidad de XMPP (Protocolo extensible de mensajería y comunicación de presencia) como posible conejillo de Indias. Incluso se propusieron ideas para avanzar de forma prudente en el caso del DNS, como por ejemplo, no enviando preguntas completas hacia arriba en la cadena del DNS.

Pedidos de no convertir el "estándar a prueba de disidentes" en el estándar común / "¡Legalícenlo!"

Del otro lado del considerable interés en la tarea de refuerzo de seguridad, existe una preocupación por la recarga innecesaria de la infraestructura y de los aparatos (o usuarios). Steve Kent (BBN), por ejemplo, advirtió durante la sesión de discusión sobre STRINT que las necesidades de "unos pocos pobres hombres" no deberían convertirse en el requisito estándar (y, así, sobrecargar a todos en complejidad y latencia). La Oficial Principal de Tecnología de Internet de ISOC, Leslie Daigle, reaccionó señalando que nunca podía saberse si uno mismo no era uno de esos pobres hombres.

Uno de los problemas que se discutió bastante (por una serie de razones académicas u operativas) fue el de monitorización del tráfico. En un documento sobre STRINT, Jan Seedorf (NEC Labs) y otros enfatizaron la

"necesidad de superar el paradigma amigo-enemigo". Existe un conflicto entre la protección contra la vigilancia permanente y las operaciones simples de los proveedores de servicios, tales como proxies, utilizar cortafuegos o supervisar el desempeño. El documento propone, fundamentalmente, permitir operaciones específicas en el tráfico transmitido, utilizando potencialmente encriptación homomórfica. Seedorf dijo que quizás sería posible modificar solo partes del tráfico seguro.

Durante una excelente sesión de introducción del IETF sobre la privacidad en los protocolos, que se realizó el domingo, varios participantes reclamaron una "manera legal" de interceptar el tráfico para impedir que se hiciera de manera "ilegal".

El GT sobre el DNS necesita más reuniones de trabajo

Hace un año, parecía que no quedaba mucho por hacer en los GTs vinculados con el DNS. Las especificaciones para el DNSSEC (extensiones de seguridad para el sistema de nombres de dominio) estaban listas, aunque la adopción está lenta. Las especificaciones para DANE se completaron, y el GT de Operación del DNS estaba deliberando acerca de qué hacer con algunos documentos antiguos. El "DNS Discovery" y el nuevo intento de elaborar una estructura y un protocolo para Whois pasaron a ser discutidos en otros grupos de trabajo. No obstante, después de Snowden todo parece haber cambiado, incluso en el DNS. No solo se organizaron dos sesiones para hablar sobre la privacidad en el DNS, sino que, además, en el GT de DNSOP (Operaciones del Sistema de Nombres de Dominio) se discutió intensamente acerca de los pedidos de nuevas zonas de nombres de dominio (que de alguna manera, también fue una reacción a las revelaciones acerca de la vigilancia). Ahora parece que el GT sobre el DNS tiene un año ajetreado por delante, con nuevos Grupos de Trabajo que son de interés para los expertos en fronteras del DNS y el trabajo en marcha sobre Descubrimiento de Servicios del DNS.

Privacidad del DNS: "El DNS genérico es vulnerable al espionaje"

Las revelaciones de Edward Snowden impulsaron a los expertos en el DNS a repensar cuestiones de privacidad dentro de ese sistema. Se presentaron gran cantidad de documentos preliminares en una sesión BoF sobre encriptación en el DNS (DNSE), la cual, a pesar de que se había dicho que no llevaría a la formación de un GT, debió extenderse a una segunda sesión. A partir de dos planteamientos del problema elaborados por Stéphane Bortzmeyer (AfNIC) y Peter Koch (DENIC), el grupo utilizó parte del tiempo para conversar sobre posibles soluciones para fortalecer la confidencialidad y la privacidad en el DNS.

Planteamiento del problema

En principio, los problemas son bien conocidos (para descripciones actuales, véase Koch y Bortzmeyer). Las consultas vinculadas con el DNS se transmiten sin encriptar, y pueden ser leídas y almacenadas fácilmente a lo largo de la ruta y/o en los puntos finales. DNSSEC agregó la autentificación al tráfico en el DNS, pero no confidencialidad. Además, la adopción de la validación DNSSEC ha sido muy lenta y solo ahora, debido al aumento del interés en el uso del DNS como base para todo tipo de material de claves o certificados, puede ser que se dé otro paso adelante (véase también el informe sobre DANE más abajo).

Los datos fácilmente accesibles del DNS pueden incluir direcciones de origen de IP, u otra información identificable individualmente relacionada con el pedido de consulta. Koch arguyó que, a pesar de la declaración ampliamente aceptada de que lo que está en el DNS es público, el hecho de que alguien acceda a cierto contenido no lo es. Los sitios de partidos políticos o de alcohólicos anónimos, entre otros, son públicos, pero los usuarios pueden no querer que se los observe ingresando al sitio en un determinado momento.

Además, las consultas suceden sin que aquellos se den cuenta, por ejemplo, mediante la verificación de direcciones por parte del software de filtrado local para detectar spam u otro tráfico indeseado, o debido a consultas desencadenadas por software de correo electrónico cuando un usuario navega por los mensajes de spam en su bandeja de entrada.

Finalmente, aunque estas debilidades del DNS han existido desde siempre, pueden ahora convertirse en un punto de interés para los espías si es que se adoptan medidas de encriptación en otros protocolos, por ejemplo, para el tráfico web (con https).

Espacio de soluciones

En el BoF sobre DNSE y el adicional sobre Privacidad en el DNS se exploraron algunas posibles soluciones, y ya hay varios documentos preliminares en circulación. Las principales preguntas fueron las siguientes:

¿Pueden reutilizarse los protocolos del IETF existentes (TLS, DTLS, IPSEC) para proteger el tráfico en el DNS?

¿Hacen falta nuevos protocolos?

¿Es posible producir cambios en las operaciones del DNS para reducir el espacio de vulnerabilidad y/o aumentar la privacidad?

¿Cuáles son los efectos adversos de las medidas de defensa del DNS?

¿Qué costos adicionales se deben considerar?

En su presentación sobre el uso de DTLS e IPSEC, Eric Rescorla concluyó que el IPSEC (Protocolo de Seguridad de Internet) probablemente no funcionaría, pero la DTLS (Seguridad de la Capa de Transporte de Datagramas) podría ser una opción. Es necesario pensar soluciones para distintas partes de la cadena: equipo del cliente final hacia resolver vs. resolver hacia servidor de nombre autoritativo. Los diseños del tipo de anycast, por ejemplo, obstaculizarían la encriptación basada en la sesión.

En general, varios documentos preliminares (incluyendo los de Bortzmeyer, Mankin y Wijngaards) propusieron la utilización de la TLS, tanto autenticada como no autenticada (oportunista), como un camino viable. La propuesta de VeriSign Labs y de la Universidad de California del Sur (Mankin et al.) es utilizar DNS-sobre-TLS-sobre-TCP (para evitar el problema de la fragmentación del UDP). Esta propuesta requiere que clientes y servidores activen un bit en los campos de indicadores de EDNSo OPT meta-RR. El bit TLS-OK (TO) indicaría la habilitación de una sesión de TLS. El borrador de Mankin no trata el tema de la autenticación de los certificados. Argumenta brevemente que la encriptación oportunista (conexiones sin CA o validación basada en el DNSSEC) podría ser de mayor interés para el DNS que TLS-sobre-TCP.

La habilitación de DNS-sobre-TLS-sobre-TCP ya fue implementada en el resolver Unbound. Sin embargo, según Bortzmeyer, solo es segura cuando , “se canalizan múltiples consultas por el mismo canal” y “la compresión

de nombres también ha sido deshabilitada". DNS-sobre-TLS-sobre-TCP, según Koch, podría ganar aceptación no solo debido a la agenda vinculada con el tema de la privacidad, sino también porque beneficiaría la protección contra los ataques de reflexión-amplificación.

La propuesta de Wouter Wijngaards (nlNET labs) y Glen Wiley (VeriSign) exige la introducción de un nuevo RR. Argumentando que DNS-sobre-TLS (y también DTLS) implicaría una carga demasiado grande para los servidores autoritativos, estos autores presentaron un "ENCRYPT RR " que permitiría recurrir a una "clave pública" para encriptar una sesión. Las claves públicas para los distintos servidores del DNS podrían almacenarse en la memoria caché. Habrá que analizar temas como los dispositivos intermedios que obligan a abandonar la encriptación y volver a canales inseguros. Ni esta solución ni el DNS-sobre-TLS brindan una confidencialidad directa perfecta.

Además, los meta datos de las solicitudes al DNS siguen proporcionando mucha información sobre los usuarios del DNS: datos de ritmos temporales, direcciones de IP de origen y de destino, tamaño de los paquetes, conteo de registros, indicadores de encabezado, etc., Bortzmeyer señaló que si se almacenan más datos en el DNS, por ejemplo, claves privadas del PGP, podría fugarse más información.

Efectos colaterales de toda esta "magia"

Algunas ideas sobre cómo disminuir las huellas que deja el DNS podrían, incluso, agregar nuevos problemas vinculados con la privacidad. Almacenar más en la memoria caché podría por una parte ayudar a ocultar información (creando "ruido"), pero por otro lado significaría más información almacenada. Además, promover la encriptación podría alentar la concentración de servicios, beneficiando a los proveedores de servicios más grandes que pueden hacer la inversión necesaria. Por otra parte, desplazar el almacenamiento en la memoria caché y la resolución del DNS lo más cerca posible de los usuarios finales evitaría la concentración solo en algunos puntos que atraen a espías y/o interesados el análisis de grandes volúmenes de datos ("big data"). Quizás, “echar una pizca de polvos mágicos” sobretodo daría a los usuarios la impresión equivocada de que el problema ya ha sido resuelto por los proveedores. La privacidad perfecta o, incluso, casi perfecta, parece ser un problema difícil para el DNS. Algunas de las propuestas destacan que su principal objetivo es hacer que la vigilancia pasiva simple (en Internet) sea más difícil y más cara.

Los costos adicionales de estas nuevas técnicas deben ser afrontados no solo por los espías del DNS, sino también por los proveedores de servicios y sus usuarios, ya que la encriptación exige viajes de ida y vuelta adicionales. Esto resultaría en un aumento general del tráfico, debido al material de claves y contenido cifrado que circularía de un lado para otro junto con las consultas y respuestas habituales. Por cierto, las empresas que se ocupan de gestión del tráfico, venta u operación de dispositivos intermedios, o aquellas vinculadas con "big data", no están muy entusiasmadas.

Varios de los oradores se preguntaron contra qué enemigos se dirigían los esfuerzos (Russ Mundy, contratista del gobierno, Sparta) y cuál era el saldo costo-efectividad, dado que la protección a nivel del transporte solo ofrecería una protección incompleta (Ralf Weber, Nominum).

En la sesión de discusión sobre STRINT (véase más arriba) que precedió a la reunión del IETF, en una discusión sobre la encriptación oportunista en general, Steve Kent (BBN, también contratista del gobierno de EE UU) cuestionó la idea de que todos los usuarios se vieran obligados a pagar más por un nivel de protección que solo una minoría deseaba alcanzar.

Próximos pasos

La sesión sobre el DNSE y la sesión adicional sobre privacidad del DNS no llegaron a ninguna conclusión con respecto a los próximos pasos. Solo luego de la sesión oficial de DNSOP se tomó la decisión de que el trabajo sobre privacidad del DNS continuaría fuera del GT Se decidió utilizar una lista de correos más amplia que el GT (“dns-privacy”) como plataforma para conversar sobre el tema, y tratar de completar un planteamiento del problema y posibles requerimientos. A pesar del alto grado de interés en la privacidad del DNS manifestado durante el encuentro en Londres, aparentemente no es posible avanzar con rapidez. La discusión sobre el alcance que debería tener esta tarea continuará.

Nombres especiales: algo menos caros que 185.000 dólares

La discusión más delicada que sostuvo el GT sobre DNSOP durante la reunión en Londres se centró en la posible reacción a pedidos al IETF de que delegue dos conjuntos de TLDs especiales, según el procedimiento establecido en la RFC 6761 sobre "Nombres de dominio para usos especiales". La relativamente nueva RFC referida al procedimiento de estandarización, escrita por dos autores de Apple, detalla cómo considerar el agregado de dominios especiales/TLDs. Este documento afirma lo siguiente:

“De manera similar, *si un nombre de dominio tiene propiedades especiales que afectan la manera en la que las implementaciones de software y hardware procesan el nombre*, las cuales se aplican siempre, independientemente de la red a la cual esté conectada la implementación, *ese nombre de dominio puede ser candidato a ser declarado Nombre de Dominio para Usos Especiales por parte del IETF*, que especificará el tratamiento especial que las implementaciones deben darle a ese nombre. Por otra parte, si la designación de un nombre determinado como especial no resultara en ningún cambio en las implementaciones, eso indica que el nombre puede no ser especial de ninguna manera concreta, y puede ser más apropiado utilizar los mecanismos del DNS ya existentes [RFC1034] para proporcionar la delegación, los datos o la falta-de-datos necesaria para el nombre en cuestión. *En los casos en los que puede lograrse la conducta deseada mediante los procedimientos de registro de nombre de dominio ya existentes, deberían usarse esos procedimientos. La reserva de un Nombre de Dominio para Usos Especiales no es un mecanismo para eludir los procedimientos normales de registro de nombres de dominio* (las cursivas son mías).

Existiendo al menos dos pedidos recientes al IETF/IESG de que habilite los registros de dominios/TLDs para usos especiales, el organismo debe considerar cómo responder a solicitudes de este tipo.

Solicitudes al IETF/IESG para la delegación de dominios especiales

Uno de los pedidos es el resultado de estudios sobre conflictos entre nombres de dominio relacionados con la introducción de nuevos gTLDs. ICANN mismo ha dejado en suspenso varias cadenas de caracteres que, según el estudio realizado por Interisle Consulting Agency, se utilizan ampliamente como pseudo-nombres del DNS. La investigación muestra que .local recibe 10.000 solicitudes por segundo, y .home solo un poco menos.

Lyman Chapin, autor de Interisle, y Marc McFadden, de InterConnect Communications, escribieron un Borrador de Internet que solicita que localdomain, domain, lan, home, host, corp, mail y exchange sean incluidos en la lista de dominios reservados, en conformidad con la 6761. Varios de estos nombres fueron

pedidos por uno o más solicitantes en el programa de solicitudes para nuevos gTLDs. En el caso de .mail, por ejemplo, cinco de las siete solicitudes originales todavía son válidas.

El segundo pedido de que el IETF reserve TLDs fue presentado por un grupo de programadores de TOR y Gnunet que aspiran a que se habiliten lo que ellos llaman "alternativas al DNS totalmente descentralizadas e inmunes a la censura", pero por fuera del DNS. El objetivo es permitir la interoperabilidad, o en el caso de '.exit' pTLD (pseudo TLD), controlar el enrutamiento superpuesto de redes y especificar las opciones de selección de ruta [TOR-PATH] de manera segura. El grupo, que incluye al representante de TOR Jacob Applebaum, solicita la aprobación por parte del IESG de ".gnu", ".zkey", ".onion", ".exit" y ".i2p" como dominios especiales, en concordancia con la RFC 6761.

Una posible opción para el IESG/IETF, presentada en Londres por Warren Kumari (Google) y Andrew Sullivan (Dyn), es la de establecer un sub-árbol de nombres de dominio especiales .alt (de "alternativo") para dar cabida a experimentos fuera del DNS. Fundamentalmente, Kumari señaló que ha habido experimentos históricos con dominios para usos especiales, motivados por la idea de permitir el uso alternativo de cadenas del tipo de las del DNS: .bitnet, .csnet, .uucp, .oz, .free, y podrían agregarse otras. Para registrar este uso, podría utilizarse un árbol especial .alt a fin de evitar problemas. Las cadenas bajo .alt no se buscarían en el DNS. Otras medidas propuestas por Kumari/Sullivan que permitirían la distinción entre dominios pseudo- y dominios comunes son las siguientes:

1. *Los resolvers "stub" PUEDEN elegir no mandar consultas sobre nombres en el TLD ALT a ningún resolver que esté más arriba.*
2. *Los resolvers iterativos DEBEN seguir los consejos brindados en la RFC6303, Sección 3.*
3. *Los servidores de nombre de la zona raíz deben brindar respuestas NXDOMAIN, o el TLD ALT debe ser delegado a un "nuevo estilo" de servidores de nombre AS112*

Los caracteres solicitados para la comunicación que promueve la privacidad, p2p, pueden o no moverse bajo .alt, declaró Kumari. Es necesario aclarar la RFC 6761 y, además, establecer una cooperación estrecha con ICANN.

¿Eludir los procedimientos de solicitud de ICANN?

Ninguno de los recientes documentos preliminares acerca del procedimiento para solicitar TLDs para usos especiales fue presentado por sus autores. La nueva co-presidente del GT sobre DNS OP, Suzanne Woolf (ISC), quien es también miembro sin voto del Consejo de ICANN y miembro del Comité Asesor sobre el Sistema de Servidores Raíz, destacó la necesidad de que el GT analizara cuestiones de operatividad (¿cómo podemos ayudar a los operadores?) y de interoperabilidad. El GT no está en condiciones de tomar decisiones formales: eso es cuestión del Grupo Directivo de Ingeniería de Internet (IESG por sus siglas en inglés).

Joel Jaeggli, uno de los directores de área responsables del IESG, dijo que existe la preocupación de que ese tipo de delegaciones pueda "abrir las puertas de par en par a los registros especiales". De todos modos, el IESG debe analizar el tema, y no está "para nada apurado por tomar una decisión" acerca de las solicitudes existentes. Los próximos pasos en relación con estas solicitudes resultan algo delicados para la comunidad técnica. El debate que tuvo lugar en Londres indica que hay varias cuestiones que merecen atención. Aún cuando los dominios para usos especiales tuvieran que resolverse fuera del DNS, el agregado de nuevos

dominios ciertamente resultaría en una mayor fuga de consultas. Las aplicaciones pueden tener problemas con estos tipos de sistemas paralelos.

En lo que respecta al proceso de ICANN, una pregunta que surgió fue si era apropiado bloquear dominios ocupados ilegalmente (como .corp. .home y .mail). La otra, muy delicada, fue si establecer un registro paralelo en IANA para usos especiales no era simplemente una forma de eludir el procedimiento penoso (y costoso) exigido por ICANN, y si no sería un llamado a burlar el sistema, sobre todo si los dominios para usos especiales pudieran ser resueltos en el DNS.

Incluso considerando que puede ser que ICANN termine siendo el operador de IANA, este debate será interesante y sumamente delicado.

Cerrar filas: Gobernanza de Internet@IETF

En la sesión de "Actualización de la gobernanza de Internet", que parece haberse convertido en un componente habitual de los encuentros del IETF y que atrae multitudes de ingenieros, un tema crucial ocupó el centro de la escena: la posición del IETF/IAB respecto del futuro de IANA. Retrospectivamente, la discusión debe considerarse, sin lugar a dudas, como una medida para lograr consenso en la comunidad del IETF acerca de la declaración (hasta ese momento no divulgada) de organizaciones de I* y otras instituciones de operadores (incluyendo a CENTR, LACTLD, etcétera), ofrecida en respuesta al anuncio sobre IANA realizado por la Oficina Nacional de Telecomunicaciones e Información (NTIA por sus siglas en inglés) el 14 de marzo.

Durante la sesión de actualización, Olaf Kolkman (Nlnet labs) presentó los puntos principales de una declaración del IAB/IANA, que se asemejaban mucho a los argumentos centrales de la posterior declaración conjunta de I*:

- La Comunidad de Internet es capaz de ocuparse adecuadamente de los parámetros de protocolos (una tarea de IANA)
- Es una función que ICANN cumple bien (no hay necesidad de cambiar los roles)
- Principios operativos ("modelo multi-actor"): apertura, transparencia, rendición de cuentas
- La arquitectura de Internet necesita registros que funcionen bien
- Cambios de la función basados en las RFCs
- El IETF continuará liderando y coordinando la función de administración de los parámetros de protocolos como componente integral del proceso de establecimiento de estándares del IETF, así como el uso de los protocolos resultantes (el IETF controla su destino).

A pesar del amplio consenso despertado por la declaración (un voto sonoro de claro apoyo a la postura en general), durante el periodo de discusión se plantearon varias cuestiones en relación con la **propiedad/los derechos de autor de los datos** registrados en el registro de parámetros de protocolos y, asimismo, con la posibilidad de que el IETF **cambie el proveedor** en el futuro.

El principio correspondiente en la RFC 6220 es que el IAB "tiene la responsabilidad de definir y gestionar la relación con el Operador de Registros de Protocolos", incluyendo "la selección y gestión del Operador de Registros de Parámetros de Protocolos", etc. Aun cuando algunos participantes en la sesión se mostraron

satisfechos con las declaraciones de Steve Crocker, presidente del Consejo Directivo de ICANN, quien aseguró al público en la sala que ICANN no se considera titular de derechos de autor de nada de lo que publica, otros recomendaron que se realizara una aclaración en la línea de la RFC 6220.

Hubo más comentarios críticos (véase las actas del debate completo aquí) acerca de la falta de diferenciación entre "Comunidad técnica de Internet" y "Comunidad de Internet" en los puntos centrales que se presentaron. Kolkman argumentó que la supervisión por parte del IAB y del IETF de la función de parámetros de protocolos parecía suficiente para garantizar la estabilidad. A la vez, los gobiernos podrían brindar aportes para la formulación de políticas y estándares de manera más general, un tema que debería conversarse separadamente. Finalmente, Kolkman y Housley afirmaron que el IAB podría considerar cambios a su postura, la cual, de todos modos, sería utilizada no como la "postura del IETF", sino como "orientación para las autoridades".,

Hubo algunas sutilezas ocultas en la discusión, que duró casi una hora, incluyendo un comentario de Patrick Fälström. Este recomendó una interpretación de los puntos discutidos en términos de su coherencia con la Agenda de Túnez (aprobada por la Cumbre Mundial sobre la Sociedad de la Información, CMSI) y, por lo tanto, se opuso a la realización de otra edición de una reunión plena de seguimiento de la CMSI. En este momento, las conversaciones sobre la reunión de seguimiento de la CMSI diez años después de su realización se encuentran en la etapa diplomática.

El presidente de ICANN (y uno de los autores de las primeras RFCs), Steve Crocker, describió el panorama más general, que incluye la globalización de IANA y de ICANN. Además, existe una discusión en marcha sobre gobernanza de Internet que excede a estas instituciones. Crocker consideró que una relación ICANN-IANA del estilo de la relación de proveedor (parecida a la que mantiene el IETF con el "RFC editor") no sería ampliamente aceptada.

Es interesante agregar que luego de la discusión sobre la NTIA, el presidente de ICANN, Fadi Chehadé, sostuvo que el debate sobre la globalización de ICANN/IANA sería tratado en la consulta a realizarse en la inminente reunión ICANN 49 en Singapur, mientras que el tan mencionado encuentro en Brasil estaría dedicado a temas más amplios de la gobernanza de Internet. En la conferencia de prensa que siguió al anuncio sobre la NTIA, Chehadé declaró que no era necesario tratar el futuro de ICANN allí. Queda por ver si todos los organizadores aceptarán esta postura, o si algunos la rechazarán por considerarla una redefinición.

Grupos de Trabajo, BoFs

DANE

"Si quieren implementar DANE 'a la rápida', no lo hagan". Esta fue la recomendación de Victor Dukhovni cuando presentó los documentos preliminares "Implementación de DANE TLSA y guía operativa" y "Seguridad del SMTP a través de una DANE TLS oportunista". Dukhovni, quien participa en el IETF por primera vez, trabajó anteriormente para una institución financiera y está a cargo de la seguridad en su nueva empresa. Ha implementado DANE SMTP y, además, publicó documentos preliminares acerca de temas y salvaguardias que deben tenerse en cuenta en nuevas ediciones del SMTP y de DANE BIS.

El cruce de fronteras ("proveedor de servicios de correo/servidor MX" y "proveedor de dominio" no son habitualmente lo mismo) ha impedido hasta ahora el uso de TLS para proteger el tráfico del SMTP. La implementación de DNSSEC y DANE permitió por primera vez que se usara la TLS autenticada para SMTP a MX entre partes que no habían establecido todavía una convención de identidad fuera de banda, según explica la RFC preliminar de Dukhovni (publicada conjuntamente con Wes Hardaker).

Una de las mayores dificultades para los implementadores fue la definición de hasta 24 combinaciones diferentes de parámetros de registro de TLSA, dependiendo, por ejemplo, del tipo de gestión de certificados o claves que se hubiera utilizado. En aquellos casos en los que el punto final del transporte de TLS se obtuvo indirectamente a través de SRV, MX o CNAME, la complejidad fue mayor.

Dukhovni explicó a esta periodista que al publicar las especificaciones del DANE, nadie parece haberse preocupado por la posibilidad de que el SMTP tuviera que manejarse con malos resultados por el lado de las Autoridades Certificadoras. Por ello, si se utiliza DANE TLSA con MTA o MTA SMTP, de acuerdo con su propuesta, se debe ser "consciente de la eliminación de cualquier rol de la infraestructura de clave pública (PKI por sus siglas en inglés) de las CA" (véase el documento preliminar para más detalles). Según Dukhovni, Postfix 2.11 admitía DANE TLSA, y también se estaba trabajando para lograr compatibilidad generalizada para DANE TLSA en OpenSSL y, como paso siguiente, compatibilidad con Exim. Dukhovni afirmó que conocía personalmente alrededor de 20 dominios compatibles con DANE SMTP y 30 más que ya están disponibles, y que para fin de año podría haber 100. La posibilidad de una implementación gradual con opciones alternativas es útil.

Otras presentaciones en el GT sobre DANE incluyeron panoramas a vuelo de pájaro de DANE/OPENPGP y DANE/IPSEC. Para este último hay distintas propuestas: Eric Osterweil, VeriSign y otros (véase este enlace), y Valery Smyslov, Elvis Plus (véase este enlace). La unión de OpenPGP y DANE permitiría la publicación y localización seguras de claves públicas de OpenPGP en el DNS utilizando un nuevo Registro de Recursos del DNS OPENPGPKEY. Las distintas propuestas están todavía en elaboración (véase también SMIME y DANE): se está considerando mayor protección para DANE en XMPP (véase el informe sobre el IETF de Berlín) y, ahora, también un posible uso de DANE TLSA para SIP. En este momento, parece, ciertamente, que DANE puede avanzar un poco más (y con ello DNSSEC).

Un tema que se discutió en distintos GTs que es de interés para la comunidad del DNS es el trabajo de Olafur Gudmundson sobre vocabulario del DNS y su relación con DANE.

GT sobre WEIRDs (Servicio Extensible de Datos de Registro en Internet)

El co-presidente del GT sobre WEIRDS, Olaf Kolkman, afirmó que el grupo espera terminar su trabajo incluso antes de la próxima reunión en julio en Toronto. Por su parte, el otro co-presidente, Murray Kucherawy, declaró que todos los documentos base habían sido enviados al IESG una vez y habían sido devueltos, y serían reenviados nuevamente como un sólo paquete una vez que se respondieran las preguntas abiertas en otros tres documentos. Durante la reunión en Londres, el debate se centró en el mecanismo de arranque para ayudar a localizar los servidores RDAP (protocolo de acceso a los datos de registro).

Se planteó la posibilidad de solicitar a IANA que se creara un nuevo registro para nombres de dominio, esencialmente TLDs, con las siguientes columnas: 'dominio' y 'URL RDAP'. El contenido debería estar conformado inicialmente por un extracto de la base de datos de la zona raíz [domainreg]. Los registrantes para estas entradas tienen derecho a asignar a la columna URL RDAP un valor para su espacio respectivo, utilizando los mismos canales de comunicación ya establecidos entre los registrantes y IANA.

Otros tres registros de IANA cubrirán las direcciones de IP y los números ASN. Esta opción llevó a una discusión en el GT y a una conversación en privado entre Kolkman y el director de área, Pete Resnick. Kolkman resumió el resultado durante la sesión: "Existe preocupación con respecto al uso de la sección de "Consideraciones a IANA" para crear registros con una política y control de nombres. Hay maneras de que nos puedan sacar de ahí". Resnick declaró que el GT podría elaborar un formato para registros y entradas, pero no debería tocar el mecanismo de ingreso de datos en los registros.

No hay necesidad de esperar a la publicación final del Grupo de Expertos en Whois de ICANN, afirmó Scott Hollenbeck (VeriSign), uno de los autores de las especificaciones de WEIRDS y miembro del grupo de expertos. RDAP (acceso y preservación de datos de investigación) tendría suficiente apoyo. En el futuro podrían realizarse las extensiones necesarias (a pesar de que la información solicitada por ICANN ya está cubierta con el Whois).

Es interesante observar que el GT sobre WEIRDS no trató el tema de privacidad del DNS. Los autores (y la mayoría del GT) parecen pensar que los registros podrán elegir qué datos pueden brindar para responder consultas sobre WEIRDS y qué datos no. No se estableció una relación con los problemas ya experimentados por los registros localizados en jurisdicciones con normas de privacidad más estrictas cuando intentaron registrar exenciones de obligaciones contractuales vinculadas con Whois. Las consultas sobre nombres asociados con direcciones de IP específicas, por ejemplo, pueden verse afectadas por cuestiones de privacidad.

SAAG (Grupo asesor del área de seguridad)

Se ha hablado mucho acerca de la necesidad de encontrar procesos alternativos para elegir cifrados nuevos luego de que el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) tuvo que reconocer que su propio procedimiento (la elección de un generador de números aleatorios) había sido influido por una de sus "partes interesadas": la Oficina de Seguridad Nacional (NSA, por sus siglas en inglés).

El Crypto Forum Research Group (CFRG), del Internet Research Group, debatió la posibilidad de que el IETF organizara concursos parecidos a los del NIST. Kevin Igoe (NSA), co-presidente del Internet Research Task Force (Equipo de tareas sobre investigación en Internet) (IRTF), informó brevemente sobre la discusión del CFRG durante la reunión del SAAG, confirmando el pedido de organizar concursos en el IETF/IRTF.

Sin embargo, Igoe sostuvo que al IETF/IRTF le sería difícil financiar un concurso, ya que el NIST había invertido 25 años-personas de trabajo y gastado alrededor de 2,5 millones de dólares en el concurso de algoritmos que se había realizado recientemente. Si bien los representantes del NIST en Vancouver también indicaron que organizar concursos requería mucho trabajo experto, en Londres uno de los representantes le dijo a esta periodista que utilizar cifrados elaborados en otros lugares sería una opción para el NIST, porque el proceso y la calidad de los cifrados se ajustarían a los estándares aceptados.

La sesión de trabajo sobre STRINT, de hecho, incluyó una reflexión acerca del trabajo del IETF sobre nuevos algoritmos como una tarea por realizar. Un experto le dijo lo siguiente a esta periodista: "El NIST

se equivocó, y el NIST es demasiado lento". Recién hace poco tiempo solicitó comentarios públicos acerca de su trabajo de estandarización de cifrados. Durante la reunión del CFRG, se mencionó repetidamente que el IETF no tiene suficientes conocimientos sobre encriptación. Asimismo, se consideró que la necesidad de una cooperación más estrecha de este organismo con la Comunidad Crypto debería ser la primera medida a tomar. Se decidió incrementar la comunicación con esa comunidad.

David McGrew, uno de los co-presidentes, afirmó que dicha comunicación era necesaria, y que las próximas reuniones del CFRG podrían realizarse paralelamente a los congresos de la Asociación Internacional para la Investigación Criptológica (IACR por sus siglas en inglés). Dan Gillmore, por su parte, sostuvo que los concursos de cifrado habían recibido comentarios positivos por parte de miembros del IETF/IRTF durante el Taller sobre Criptografía en el Mundo Real en enero. Dichas actividades podrían acercar más expertos en encriptación al IETF. Considerando el nivel de interés expresado por los expertos, no ha habido mucha discusión franca y abierta en Londres.

Russ Housley, presidente del IAB, presentó un trabajo sobre la agilidad criptográfica. Una nueva RFC abordará la manera en la que el IETF da lugar a la agilidad para pasar de algoritmos más débiles a algoritmos más fuertes, preferentemente sin cambiar las especificaciones de base. Los algoritmos serán identificados mediante identificadores registrados en un registro de IANA.

BoF sobre fronteras dentro de dominios

Una sesión BoF sobre "Fronteras entre dominios" exploró posibles alternativas a la lista "public-suffix" (lista pública de sufijos). La lista, que es administrada actualmente por la Mozilla Foundation, es una lista de sufijos (TLDs de ICANN o de privados) que incluye comodines y excepciones. Según la presentación de Gervase Markham, de Mozilla, esta lista es utilizada principalmente por las empresas creadoras de navegadores para implementar distintas políticas en la gestión de cookies, la comunicación entre páginas Web, la transparencia para proteger contra ataques de suplantación de identidad, etc. También la usan terceras partes, por ejemplo, para los Requisitos Básicos del CAB (para evitar comodines excesivamente amplios), DMARC (Autenticación, Información y Conformidad de Mensajes a través del Dominio, para mecanismos anti-spam), usos que se documentarán en un WIKI especial. Según Markham, el denominador común es "qué bits de la red son propiedad por una entidad común".

Los problemas mencionados en el BoF (y las razones por las que este se creó) incluyeron temas como rapidez en actualización, y completitud de datos; así como falsos positivos y negativos. Justo antes del BoF, por ejemplo, se agregaron tres nuevos gTLDs a la raíz, pero no se veían inmediatamente en la Lista de Sufijos Públicos. También surgieron preguntas sobre la modalidad de procesamiento de los cambios y las políticas que se habían formulado para estos procesos.

Yngve N. Pettersen (Opera), Andrew Sullivan (Dyn) y John Levine (Taughannock Networks) presentaron documentos preliminares sobre posibles alternativas. Los tres buscan algún tipo de opción orientada hacia el DNS con registros (RRs) nuevos. No obstante, también se consideró una simple medida de mayor formalización y estandarización de la misma lista public de sufijos públicos actual.

Sin mayor claridad sobre el alcance del problema, se estableció un grupo de diseño integrado por cuatro autores (Olafur Gudmundson, Murray Kucherawy, Ed Lewis y Jothan Frakes) y los presidentes del BoF para analizar las siguientes preguntas:

- ¿Estamos estandarizando la funcionalidad de la Lista de Sufijos Públicos? Y, ¿qué casos deberían ser admitidos como mínimo?
- ¿Cuáles son las partes que participan en la provisión de información? ¿Cuáles son sus respectivas funciones, responsabilidades y facultades?
- O, según las preguntas de Joe Hildebrand, ¿de dónde vinieron los datos, cómo se transmitirían, cómo se establecería su autoridad y cuál es la relación con el modelo de seguridad de la red?

Puede encontrarse una lista de discusión para DBOUND (Fronteras dentro de Dominios) aquí.

Novedades del IETF

El encuentro en Londres también fue utilizado por otras organizaciones de I* para cerrar filas (véase, por ejemplo, la exposición apasionada de Fadi Chehadé, que destacó la función de ICANN en este proceso) y para marcar la entrega de mando de ISOC por parte de Lynn St. Amour a Kathryn Brown, ex-vicepresidente principal de elaboración de políticas públicas y responsabilidad empresarial de Verizon.

Nueva presidente de ISOC / Internet@parliament

St. Amour fue muy aplaudida por los ex-presidentes del IETF y el IAB, y ovacionada de pie por los participantes en la sesión plenaria. La ex-presidente deja un ISOC que ha crecido mucho. La nueva presidente viene desde afuera con algunos cambios en mente; le dijo a esta periodista que la cooperación con los distintos Capítulos de ISOC era un tema en su lista. En su discurso inaugural, Brown prometió que ISOC estaría presente en los próximos debates sobre gobernanza de Internet. Delante de miembros del parlamento británico, enfatizó fundamentalmente la necesidad de reunir a todas las partes interesadas alrededor de la mesa de elaboración de nuevas leyes y normas para Internet.

En la reunión, organizada por el Capítulo Británico de ISOC y Afilias en el parlamento durante la semana del IETF, también se escucharon declaraciones interesantes por parte de algunos parlamentarios, entre ellos, un miembro de la Comisión Conjunta de Inteligencia y Seguridad, George Howarth (Partido Laborista), un miembro de la Comisión de Derechos Humanos, Julien Huppert (Partido Demócrata Liberal) y el político conservador David Davis. Davis y Huppert fueron sumamente críticos de las reacciones del gobierno al caso de espionaje. Davis dijo que Whitehall era "incompetente". Howarth, por su parte, reconoció la necesidad de transparentar el trabajo de los servicios de inteligencia, y señaló, a la vez, que era necesario luchar contra el terrorismo y la pornografía infantil. El legislador laborista declaró que el debate acerca del equilibrio entre seguridad y libertad personal recién empezaba.

ICANN anfitrión del IETF, continuará el debate sobre gobernanza de Internet.

ICANN fue el anfitrión del IETF 89, por lo cual Chehadé ofreció la habitual presentación del anfitrión durante la plenaria administrativa. El presidente habló sobre el servicio prestado por ICANN al IETF, la función de IANA, bajo un acuerdo de niveles mínimos del servicio. Asimismo, aplaudió la tarea del Foro y lo definió como un referente para el modelo multi-actores. Mencionó, además, las inminentes discusiones que tendrán lugar en

Brasil y otros eventos. La "comunidad técnica/operativa de Internet" vuelve a Londres este año: durante la reunión de ICANN en Londres, a realizarse en junio, se planifica una reunión de gobierno de alto nivel.

Un frente unido de I*

Además de la necesidad de aumentar la seguridad (véase más arriba), Arkko mencionó los próximos debates. Reiteró que el IETF tiene que hacer más divulgación, y dijo que "los gobiernos se han dado cuenta de que esto de la Internet no va a desaparecer". Eventos tales como la reunión del Internet@parliament empiezan a volverse más comunes, incluso para la comunidad de ingenieros.

En conclusión, las organizaciones de I* se presentaron como un grupo sólido en relación con cuestiones operativas (IANA) y, además, en el frente de política y diplomacia. La asistencia al IETF en Londres fue alta: 1.364 participantes de 60 países (comparada con 1.115 de 51 países en Orlando).

El próximo IETF (IETF 90) tendrá lugar en Toronto del 20 al 25 de julio.