INFORME IETF 94

Yokohama

2-6 noviembre 2015

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/document/4601

LACTLD
Latin American and Caribbean ccTLDs Organization

Índice

IETF94 a 3.000 metros

Resumen ejecutivo

El IETF94 en Yokohama se caracterizó por una extensa discusión sobre las mediciones y sus posibles beneficios para la elaboración de protocolos. La facilidad de acceso a los datos de las interconexiones, mencionada por algunos participantes, ocasionaría problemas de privacidad, según se advirtió durante un intenso debate en la plenaria. El Grupo de Trabajo de Investigación en Internet (IRTF por sus siglas en inglés) organizó un taller sobre mediciones antes del foro, simultáneamente con la reunión del Grupo de Interés Especial ACM sobre Comunicación de Datos (SIGGCOM por sus siglas en inglés).

La conexión del trabajo de IETF/IRTF con el de otros organismos parece estar convirtiéndose en una tendencia. Durante la reunión, se encontraron representantes del sector de telefonía móvil (GSMA) y de IAB/IETF para decidir cómo continuar la tarea llevada a cabo en septiembre en un taller conjunto que investigó el aumento del tráfico encriptado en las redes. GSMA también está considerando dar acceso a los datos a los interesados en mediciones (véase, en particular, el Grupo de Investigación sobre HOPS).

El trabajo del IETF y las posibles "transiciones" desde los protocolos preexistentes a los nuevos (tanto técnicos como organizacionales) se refleja en un documento preliminar escrito por Dave Thaler. También están en marcha modificaciones del formato de las reuniones. A partir de la introducción de una reunión intensiva sobre códigos (Code Sprint) y de la hackatón (además de “Bits y Bytes”), el IETF redujo el tiempo de las plenarias mediante la combinación de la administrativa y la técnica.

En 2016, el IETF se reunirá por primera vez en Latinoamérica, y está dispuesto a gastar más de lo habitual para avanzar hacia la internacionalización y la diversidad. Otra expresión del cambio en esta organización, que solía estar conformada solamente por gente del ámbito de la tecnología, es la creación inminente de un Grupo de Investigación sobre Derechos Humanos bajo la égida del IRTF.

En cuanto al Sistema de Nombres de Dominio, está en marcha la revisión de la 6761, dirigida por un equipo de diseño. El Grupo Directivo de Ingeniería de Internet (IESG por sus siglas en inglés) quiere que la comunidad "arregle" la 6761, dijo el presidente del IETF, Jari Arkko, durante la plenaria. En esencia, existe una preocupación dentro del IETF de que la organización pueda ser (ab)usada como proveedora alternativa de un espacio de nombres (véase el apartado sobre nombres especiales).

DNS sobre TLS está acercándose a la última llamada (véase el informe del GT sobre DNSPrive). Mientras tanto, se está impulsando nuevamente el agregado de confianza mediante el registro de la raíz firmada de DNSSEC.

Destacados

El IETF y la reserva de nombres especiales: más importante imposible

La RFC 6761, que se ocupa de los nombres especiales, será revisada por un Equipo de Diseño recién creado. Sus miembros fueron elegidos por los presidentes del grupo de trabajo DNSOP y confirmados durante la reunión en Yokohama. Estos son Ralf Droms (el único que no está vinculado con el DNS), Alan Durand (ICANN), Peter Koch (Denic) y Joe Abley (Dyn). Salvo Droms, que fue nombrado por sugerencia de la co-presidenta del GT Suzanne Woolf, se trata de los autores de una presentación sobre una posible revisión del Registro de Nombres Especiales del IETF.

Selección del equipo de diseño

Durante la reunión del GT, se hicieron comentarios acerca de la falta de claridad en la comunicación sobre el proceso de selección. Los presidentes del GT no habían dado seguimiento al pedido de un número no divulgado de personas de formar parte del equipo. Suzanne Woolf se disculpó. La conformación del grupo (dos personas de ICANN, o cercanas a ICANN, y un ex-presidente del GT que había manifestado reservas sobre el tratamiento de los nombres especiales) favorece un resultado más conservador.

El proceso de la tarea de diseño

Durante la reunión del grupo de trabajo en Yokohama, no quedó del todo claro de qué manera este estaría involucrado en los próximos pasos. Según la explicación de Droms, el equipo de diseño realizaría la tarea de revisión, informaría al grupo de trabajo e impulsaría el debate en la lista de correos, en lugar de encontrarse en persona durante las reuniones del IETF. Por otra parte, el Presidente de la Junta de Arquitectura de Internet (IAB por sus siglas en inglés), Andrew Sullivan, definió la revisión de la RFC 6761 como "más importante imposible" para el GT y, por ello, consideró que "merece el tiempo y la atención de la gente que quiera asistir".

Tampoco está muy claro cómo procederá el GT a partir de ahora, pero, dados el considerable interés y los comentarios suscitados en el IETF (también por parte de Jari Arkko, quien dijo que el IESG le había devuelto el tema a la comunidad para que encontrara una solución), se asignará tiempo para la discusión. Otros documentos preliminares, entre ellos, .bit (bitcoin) y .gnu (Sistema de Nombres de Gnu), fueron postergados por el momento.

La esencia de la cuestión: aspectos arquitectónicos, técnicos y organizacionales

Durante su presentación de un documento preliminar de planteamiento del problema, Koch y Durand afirmaron que pensaban estudiar la 6761 desde una perspectiva arquitectónica, técnica y organizacional. Desde el punto de vista arquitectónico, se reconoce que el espacio de nombres no es simplemente el sistema de nombres de dominio, sino que hay otros tipos de nombres que utilizan protocolos más o menos diferentes. Localhost permite la resolución interna de nombres (sin referencia al DNS), DNS Multicast utiliza Local y Onion se usa “para construir nombres que designan servicios ocultos anónimos que pueden contactarse a través de la red Tor utilizando el

enrutamiento de onion".

En estos casos, los TLDs no se emplean como tales, sino como “conmutadores para protocolos" (del DNS a otra cosa), y se consideraría la posibilidad de catalogarlos o utilizar un .alt como indicador para el conmutador que permite optar por resoluciones alternativas. En términos técnicos, la pregunta es cómo harán los usuarios para saber cómo tratar los nombres especiales a fin de evitar posibles problemas, por ejemplo, el filtrado de .onion o de otros nombres que no son del DNS. En el caso de .onion, podrían producirse problemas de privacidad/seguridad para sus usuarios.

¿Un conflicto entre la RFC 6761 y el MdeE entre el IETF y ICANN (RFC 2860)?

Desde el punto de vista organizacional, la RFC 6761 habría modificado, en cierta medida, la relación entre el IETF y ICANN. Con la RFC 2860, el IETF se apropió de la función de órgano de formulación de políticas para el DNS y ICANN, y este último adoptó un proceso para delegar nombres, aunque complicado y costoso. Durand afirmó que se estaba considerando un segundo llamado abierto para solicitudes de TLDs.

Mientras que el MdeE había hecho una excepción, si bien vaga, de la prerrogativa de ICANN como órgano a cargo del espacio de nombres, la RFC 6761 cambió esto ligeramente. Su revisión debería considerar los problemas intra-organizacionales (el hecho de que el IETF no tenga un proceso para reservar nombres debido a la vaguedad de la RFC) y los inter-organizacionales (¿es la 6761 una violación del MdeE?). Las preguntas acerca de la posible falta de validez de la 6761 fueron descartadas sin más porque podrían llevar a una discusión interminable. Asimismo, Arkko rechazó rápidamente la apertura de la 2860 para renegociar las funciones de ICANN y el IETF. (El IESG le pidió al GT que estudiara la 6761. La RFC 2860 no está en discusión.)

Posibles resoluciones

Las opciones que se presentaron incluían la revocación del proceso de la 6761, que no estaba incluida en el documento preliminar, como señaló Stéphane Bortzmeyer (AFNIC). Bortzmeyer urgió al equipo de diseño a volver a esta RFC para llenar los vacíos en el proceso. De este modo, la reserva de nombres especiales por razones técnicas podría entrar en funcionamiento. Otra opción sería la creación de una Zona-TLD especial (como .alt; véase la propuesta de Warren Kumari, de Google). Sin embargo, eso aún haría necesario un proceso para decidir qué reservas otorgar.

Control en lugar de confianza: el registro DNSSEC

El GT sobre Escribanía Pública para la Transparencia (Public Notary Transparency, o TRANS) está preparándose para enviar su especificación básica sobre Transparencia de los Certificados (la RFC 6962 bis) a la última llamada del Grupo de Trabajo (ULGT) en diciembre. Para monitorear los registros, el GT adoptó un documento que propone tres mecanismos para detectar conductas inapropiadas (véase el documento preliminar sobre Gossip): controlar los Sellos de Tiempo de los Certificados Firmados (SCT por sus siglas en inglés), agrupar los Árboles de Hash Firmados (SHT por sus siglas en inglés) en servidores https y, finalmente, que los clientes de http compartan directamente SCTs y STHs con auditores de confianza.

La transparencia de los certificados (AC) permitirá que los registros públicos de certificados editados por una AC sean revisados por terceros para detectar certificados falsos. Próximo a terminar la especificación básica, el GT está investigando posibles escenarios de ataque y, además, la extensión de la transparencia mediante un mecanismo de registro más allá del sistema de AC. En particular, un "BoF en el bar" (reunión informal fuera de programa) consideró empezar a trabajar con firmas de registro DNSSEC (DS).

Extender la transparencia de los certificados a DNSSEC

El registro como recurso para permitir el monitoreo de firmas ha sido descripto desde el principio como un mecanismo general. Durante el encuentro en Yokohama, una docena de personas se reunieron para conversar acerca del posible uso de registros públicos de firmas de DNSSEC para facilitar el control del uso inapropiado de claves por parte de un dueño de zona. Según un primer documento preliminar, el escenario del ataque sería el siguiente:

“Un dueño de zona que ha sido comprometido u obligado por un tercero puede secuestrar una zona hija para devolver datos de DNS diferentes, indistinguibles de los datos validados de DNSSEC de la zona hija, utilizando su propia DNSKEY para firmar datos de DNS en nombre de la zona hija. Podría entregar estos datos modificados del DNS solo a regiones o individuos escogidos, haciendo que este ataque sea muy difícil de detectar por parte de la zona hija legítima".

El primer documento preliminar, escrito por Daniel Kahn Gillmor y otros, fue publicitado muy brevemente en el GT TRANS. La discusión se trasladó a un BoF en el Bar, donde los participantes estuvieron de acuerdo en que un primer paso para poner a prueba un mecanismo debería realizarse en la zona raíz central para evitar complicaciones de zonas más grandes como .com, que podrían requerir la cooperación de un proveedor privado como VeriSign. Kahn Gillmor afirmó que el mecanismo permitiría detectar posibles versiones desdobladas de la zona raíz firmada.

En general, los mecanismos de transparencia solo permiten detectar, no prevenir. Según la propuesta del documento preliminar, los dueños de zonas deben presentar los registros de recursos DS a uno o más registros preferidos antes de publicarlos (las entradas del registro deberán ser firmadas para su autenticación). Estarían acompañados de registros de recursos adicionales (RRs de DNSKEY, de DS y de RRSIG). Un RR DS aceptado resultaría en su inclusión en un registro de monitoreo.

Wes Hardaker (Sparta) estuvo de acuerdo en que es posible ingresar todo lo que la raíz firma en el registro, si bien no está seguro de que se pueda ampliar para su adaptación a zonas grandes como .com. En el caso de la zona raíz, debido a la presencia de monitoreo intenso, cree que no se detectará nada. No obstante, registrar la raíz sería una buena prueba de concepto para el registro DNSSEC.

Co-firmas

Bryan Ford, del Instituto Suizo de Tecnología de Lausana, argumentó que el registro público (para certificados PKI o firmas DNSSEC) no es suficiente, ya que un atacante poderoso podría lograr acceso a la clave privada del AC y del servidor de registro, que no son más que puntos

únicos de ataque. Ford presentó la idea de testigos para el registro. Los cambios que no hubieran sido co-firmados por todos los testigos, que podrían ser organizaciones externas como EFF o CCC, podrían ser detectados y expuestos por dichas organizaciones. Nuevamente, todavía podría haber manipulación, pero sería detectada. El co-firmado puede, en principio, compararse con las claves PGP públicas co-firmadas.

Ford declaró que se puso a prueba una implementación de este concepto con Google que reveló que el tiempo de computación era razonable. Ciertamente, todavía existen problemas, como el manejo desprolijo de la revocación de certificados. En 74 escaneados completos de HTTPS de IPv4, los investigadores hallaron que un 8% de los certificados entregados habían sido revocados, y que obtener información sobre la revocación de certificados a menudo puede ser caro para los clientes, tanto en términos de latencia como de ancho de banda. El control de 30 combinaciones distintas de navegadores y sistemas operativos reveló que los navegadores muchas veces no se molestan en verificar si los certificados fueron revocados (incluyendo navegadores para teléfonos celulares, que nunca controlan). En Google Chrome, el CRLSet solo cubre un 0,35% de todas las revocaciones.

Según Ford, las motivaciones para que los proveedores de certificados adopten los conceptos más onerosos del mecanismo de co-firmado podrían ser la competencia, la posibilidad de disuadir a las autoridades interesadas en claves (porque sin el co-firmado, se notaría el desdoblamiento) y el poder de mercado de las compañías de navegadores (no aparecen en Chrome si no están co-firmados).

Talleres y BoFs

El GT sobre EPPEXT se transforma en GT sobre REGEXT

El grupo de trabajo sobre Extensiones al Protocolo de Aprovisionamiento Extensible (EPPEXT por sus siglas en inglés) se halla en plena modificación de su acta constitutiva y está estableciendo nuevas metas, entre ellas, posiblemente cuatro o cinco lotes de nuevas extensiones (véase la lista). El GT seguirá debatiendo las extensiones al EPP (introducidas por los operadores de registros) que se convertirán en propuestas de documentos de estandarización. Las extensiones exclusivas, o las presentaciones individuales que aspiran a recibir un estatus informacional o experimental, pueden solicitar ser incluidas en el registro EPPEXT luego de una evaluación por parte de expertos, según la RFC 7451.

Grupo 1 de ULGT, a finalizar para febrero de 2016:
-aviso de cambios externos via poll (draft-gould-change-poll)
-mapeo de epp-rdap (draft-gould-epp-rdap-status-mapping)
-extensión para revendedor (draft-zhou-eppext-reseller and draft-zhou-eppext-reseller-mapping)

Grupo 2 de ULGT, a finalizar para mayo de 2016:
-código de verificación (draft-gould-eppext-verificationcode)
-mensajes sobre el servicio (draft-mayrhofer-eppext-servicemessage)
-mapeo de verificación de nombres (draft-xie-eppext-nv-mapping)

Grupo 3 de ULGT, a finalizar para septiembre de 2016:
-tarifas (draft-brown-epp-fees-05)
-registros agrupados (draft-kong-eppext-bundling-registration)

Grupo 4 de ULGT, a finalizar para enero de 2017:

-mapeo de tablas de IDN (draft-ietf-eppext-idnmap and draft-gould-idn-table and draft-wilcox-cira-idn-eppext)
-relé (todavía no hay documento preliminar, desdoblado de keyrelay)

Con la nueva acta constitutiva, el GT también asumirá la tarea vinculada con Protocolo de Acceso a Datos de Registro (RDAP por sus siglas en inglés) (originalmente a cargo del GT sobre Weirds). El carácter más general del GT se expresará en su nuevo nombre: GT sobre Extensión de Registros (REGEXT).

Si bien no hubo documentos preliminares oficiales, se presentaron varios documentos en la lista de correos: la primera versión del perfil de los gTLDs de ICANN y un posible documento para mapear los estados del EPP y de aquellos registrados para su uso en RDAP (incluyendo posibles brechas). Otra eventual presentación individual (probablemente a través de Barry Leiba, "Area Director") es un documento preliminar sobre depósitos de datos, que ha estado pendiente desde hace un tiempo.

¿Un GT sobre todo lo que tiene que ver con ICANN?

La breve Acta Constitutiva y el debate sobre metas reveló que existen algunas preocupaciones acerca del alcance del nuevo GT sobre REGEXT. Peter Koch (Denic) cuestionó la idea de que pueda convertirse en el nuevo GT sobre "todo lo que tiene que ver con ICANN". El IETF debería concentrarse, en cambio, en la elaboración de protocolos.

La preocupación, evidentemente, es que el IETF adjudique a ICANN un derecho especial a ofrecer todos los servicios y, a cambio, devuelva a la comunidad de registradores/registros "estándares" con el sello del IETF.

Respecto del perfil de gTLDs de ICANN, antes de la reunión, Kaveh Ranjbar (RIPE) había pedido en la lista de correos que se ejerciera cautela. El IETF no debería aceptar un documento que, en esencia, resume la "política" de ICANN hacia sus registros y registradores. Scott Hollenbeck, de VeriSign, sostuvo que los requisitos de implementación (basados en el consenso de la comunidad) podrían muy bien convertirse en RFCs informativas. Existe un documento preliminar similar, sometido a discusión por ICANN, sobre las especificaciones para el Centro de Validación de Marcas (Trademark Clearinghouse).

Hollenbeck y Ning Kong, quienes reemplazaron a Jim Galvin, de Afilias, y Antoine Verschueren (previamente de SIDN) en la presidencia del encuentro en Yokohama, organizaron varias votaciones sonoras para evaluar si los miembros del GT sobre EPPEXT/REGEXT querían también seguir ocupándose de los registros informativos/exclusivos (o dejarlos para el proceso de evaluación por expertos), y si estaban de acuerdo en dividir las tareas ulteriores entre distintos grupos. Existió algo de desacuerdo sobre esta última cuestión, en particular, porque algunos pensaban que debía mantenerse cierta flexibilidad para permitir que se asumiera el trabajo sobre RDAP u otras tareas.

Tampoco se pudo llegar a un acuerdo sobre la adopción de una extensión para una política especial de registro de China: se plantearon preguntas acerca de cómo reaccionaría un órgano regulador chino si el GT cambiara los procedimientos. Un GT es responsable de cambiar un documento preliminar una vez que se "apropia" de este, es decir, cuando se inicia el proceso de estandarización.

Koch cuestionó los motivos para crear listas aún más largas de documentos en proceso de

estandarización del IETF para las extensiones EPP, debido a lo que llamó posibles "incentivos externos para tener etiquetas de 'en proceso de estandarización' para estos documentos, que no están alineados con los documentos del IETF". Estos incentivos podrían ser económicos (bonificaciones por RFCs por parte de las empresas) o un posible interés en aumentar la legitimidad de soluciones técnicas u organizacionales. Se espera que la próxima extensión a adoptar sea el documento sobre relé de claves, que prevé un mecanismo para intercambiar claves de DNSSEC en caso de cambio de registrador.

DPRIVE: Cuenta regresiva para DNS sobre TLS: ¿Y qué hay de la implementación?

El principal proyecto de protocolo del GT sobre DPRIVE, DNS sobre TLS, se encuentra en la etapa de última llamada, y debería convertirse en RFC a comienzos del año próximo. Básicamente, el GT acordó sacar los perfiles (se los tratará en un documento adicional) y StartTLS del documento. Por ahora, no habrá opción para pasar de una sesión de DNS sobre TCP a una de DNS sobre TLS. Se acordó que este cambio haría que el protocolo fuera más sencillo y "ligero".

Los servidores habilitados para DNS sobre TCP escucharán un nuevo puerto que se reservó con la IANA (Puerto 853) para la negociación de una conexión TLS. Idealmente, se podrá consulta el mismo documento para TLS y DTLS (este último fue dejado de lado como documento independiente, como puede verse más abajo). Queda por explorar el uso de otros mecanismos de autenticación aparte de TLS, por ejemplo, DANE. Asimismo, la autenticación de los clientes (además de la de los servidores) podría desarrollarse en más detalle.

Quedan dudas sobre algunos implementadores posibles. Wolfgang Beck, de Deutsche Telekom, preguntó acerca del número de sesiones paralelas que podían realizarse, ya que para DTAG realizan un millón por servidor. El documento brinda algunos consejos respecto de la mejora del desempeño, según Duane Wessels (de VeriSign Labs y uno de los autores). Christian Huitema, de Microsoft, señaló que la implementación para proveedores a gran escala sería ardua, y que existía la posibilidad de que surgieran problemas de seguridad al combinar la seguridad para un gran número de credenciales. Respecto de la implementación, Sarah Dickinson informó que Unbound se realizó con DNS sobre TLS (desde el 1 de abril de 2012). Las herramientas disponibles son digit y getdns. El equipo de privacidad del DNS ganó un premio durante la hackatón del IETF que precedió a IETF 94.

Los resultados de la hackatón que puede consultarse incluyen:

Temas de privacidad del DNS:
– extensión getdnsapi (depuración de llamadas) implementada con cambios para que los usuarios puedan conocer resultados de transporte/privacidad
– elección de privacidad edns0-client-subnet
– opción edns0-padding (el lado del cliente está terminado)
– Verificar TLS en el Recursivo - aplicación node.js

Temas de DNSSEC
– eludir barreras en DNSSEC – nueva extensión propuesta para getdnsapi
– CDS/CDNSKEY

Para más información, véase la lista de proyectos de la hackatón vinculados con DNS aquí.

DNS sobre DTLS ha sido dejado de lado por ahora. Se explorará la fragmentación

La posibilidad de avanzar en el desarrollo de DNS sobre DTLS fue básicamente dejada de lado luego de alguna discusión acerca de si valía la pena trabajar en ello y, a la vez, permitir la fragmentación y reensamblaje de paquetes demasiado grandes. Dan Wing presentó la versión DNS sobre DTLS – que se consideró como una posible variante de DNS sobre UDP – que favorece la privacidad. Sin embargo, Wing reconoció que, para prevenir que se recurra frecuentemente a DNS sobre TLS ("entonces, ¿para qué molestarse en tener DNS sobre DTLS?"), debería recurrirse a la fragmentación y el reensamblaje, algo que muchos consideran demasiado complicado (entre ellos, Andrew Sullivan, presidente de la IAB, y Paul Hofmann, una de las últimas incorporaciones al departamento técnico de ICANN). Wing estuvo de acuerdo en renunciar a una mayor elaboración del documento preliminar, que también incluyó un nuevo puerto de la IANA (puerto 853) para evitar problemas con dispositivos intermedios.

¿Nueva tarea relacionada con DPRIVE?

No hubo mucha discusión sobre el documento presentado por Allison Mankin sobre Evaluación de la privacidad para DPRIVE (que es un documento del GT) ni sobre un documento completamente nuevo sobre "encriptación de DNS sin estado", principalmente porque se trata de un enfoque diferente del utilizado actualmente con DNS sobre TLS.

Con un tema central casi listo – un mecanismo de privacidad para consultas en DNS – el GT también dialogó brevemente sobre qué tratar a continuación. Se propuso ocuparse de las siguientes cuestiones: proteger las consultas entre servidor recursivo y de autoridad (ya que cada vez más gente podría usar su propio resolvedor), de Bortzmeyer y Gillmor, relleno de EDNS, de Gillmor (para lo cual ya existe un documento preliminar), y mediciones para dar seguimiento a una futura actualización de DNS sobre TLS (Tim Wicinski).

Paul Hofmann (ICANN) recomendó un enfoque del desarrollo más conservador, del tipo esperar y ver. Allison Mankin (Veri-Sign Labs), en cambio, destacó que el grupo debería usar el existente interés por la privacidad en el DNS ya que, si esperaran, podrían perder el ímpetu actual.

DNSOP: una lista de nuevas propuestas

Además del gran debate sobre el proceso de reserva de nombres especiales (RFC 6761, véanse los Destacados), el grupo sobre DNSOP conversó brevemente sobre una lista de propuestas y aceptó trabajar sobre varios temas.

1. Una propuesta más antigua de Joe Abley, que ofrece un mecanismo para que un servidor de autoridad indique que las consultas "ANY" no serán admitidas para un QNAME en particular. Las consultas "ANY" pueden utilizarse con fines legítimos, como depurar o controlar el estado de un servidor de DNS. También pueden utilizarse para recuperar registros de recursos MX, A y AAAA para un dominio de correos en una consulta única. El problema es que las consultas "ANY" están siendo cada vez más abusadas para extraer conjuntos enteros de datos o, lo que es peor, para su utilización como factor amplificador en ataques de denegación de servicio distribuido. La vuelta a respuestas más cortas permite mitigar este tipo de ataque.

2. Un documento breve de Paul Wouters y Olafur Gudmundson describe un mecanismo para la señalización de cambios de estado de DNSSEC dentro de la banda. Esto posibilita que un hijo indique a un padre que active o desactive DNSSEC para su dominio utilizando CDS/CDNSKEY. Los cambios de estado pueden ser necesarios cuando un dueño de un dominio cambia de registrador. Hasta ahora, la imposibilidad de habilitar la confianza a través de un mecanismo fácilmente automatizado obstaculizaba el uso de DNSSEC a escala por parte de cualquiera que no tuviese acceso automatizado al "registro" de su padre. Si bien se manifestó alguna inquietud en cuanto a permitir la desactivación de DNSSEC por esta vía, en general se apoyó el desarrollo de este mecanismo siempre que se controlaran problemas de arranque.

3. Duane Wessels propuso una opción para la extensión del DNS (OPT meta-RR [RFC6891]) que posibilitará que los resolvedores de sistema final le informen a un servidor en una consulta de DNS qué claves de DNSSEC utilizan para validar la respuesta esperada. Esto permite medir la aceptación y el uso de nuevos anclajes de confianza y claves de firma de claves (después de una renovación de claves o de algoritmos). Se plantearon preguntas acerca de cómo se manejaría la información de caché, con alguna preocupación de que pudiera convertirse en fuente de ataque. Posiblemente, esto podría limitarse solo a la zona raíz. Una alternativa factible, en lo que se refiere al cumplimiento de la 5011 (procedimiento de renovación), podría ser un documento preliminar de Warren Kumari que no fue estudiado.

También se presentaron, pero no fueron adoptados todavía, los siguientes:

4. Un documento introducido por Shane Kerr (en representación de un grupo) que propone que se permita la fragmentación de mensajes de DNS en lugar de hacerlo en la capa de IP. Según el documento, el objetivo "es permitir que los servidores de autoridad respondan con éxito las consultas de DNS a través de UDP utilizando múltiples datagramas más pequeños cuando los datagramas más grandes no pueden atravesar la red con éxito".

5. Una propuesta para resucitar una parte de una propuesta más antigua (2010) de Paul Vixie sobre "Detener las búsquedas hacia los dominios hijos de la memoria caché en NXDOMAIN". Esto permite poner de manifiesto que, si no existe bar.domain, tampoco existe foo.bar.domain. No hubo consenso acerca de seguir adelante con la propuesta.

TCPInc: el IETF no puede decidir

Se espera que el GT sobre TCPInc recomiende seguridad oportunista adicional para las conexiones TCP pero, hasta ahora, el grupo no ha podido elegir entre dos propuestas en discusión. Las dos candidatas son TCPCrypt, elaborada por un grupo de investigadores de la Universidad de Stanford (Andrea Bittkau, Mike Hamburg y otros: véase aquí) y la Opción TCP TLS (de Erik Rescorla, de Mozilla). Según Sean Turner, presidente del GT, la principal diferencia entre las dos era originalmente que TCPCrypt estaba en el núcleo, mientras que la Opción TCP TLS sostenía que TLS ya había sido bien implementada y que los usuarios la conocían. Según Turner, Rescorla, mientras tanto, también trabajó para que esté en el núcleo. El objetivo principal – seguridad oportunista para TCP – y el concepto básico para establecer la conexión son bastante similares.[1]

[1] Establecimiento de la conexión para TCPCRYPT: "El intercambio inicial de claves funciona de la siguiente manera: cada máquina C tiene una clave pública efímera, K.C. Cuando C se conecta con un servidor S por primera vez, C elige un *nonce* al azar, N C: S elige un secreto al azar, N S: los dos intercambian los siguientes mensajes, que también aparecen en la Figura 1:

TCPCrypt ha sido desarrollada más a fondo para incluir una Opción de Negociación Encriptada en TCP (ENO). TCP-ENO es una opción para TCP utilizada durante el establecimiento de la conexión para negociar cómo encriptar el tráfico. Según la propuesta preliminar, puede implementarse de manera incremental y permite recurrir al TCP sin encriptar y atravesar dispositivos intermedios. La Opción TCP TLS también utiliza ENO con TLS 1.3. Según el presidente del GT, Sean Turner, se espera que la TLS 1.3. esté lista para fin de año, y que sea aprobada por los académicos antes de su estandarización final durante una conferencia planeada para febrero (el taller sobre TRON organizado por ISOC).

Los autores de TCPCRYPT indicaron que existe algún tipo de implementación en marcha, y pidieron que el GT tome una decisión: no pueden seguir con su trabajo sin un compromiso, debido a que se les están acabando los fondos para el proyecto. Si bien muchos expertos, incluyendo el director saliente del Área de Transporte, Martin Stiemerling, y el presidente del IRTF, Lars Eggert, urgieron al GT a elegir una de las dos soluciones, algunos están de acuerdo en que se continúe con implementaciones paralelas.

Habiendo ofrecido al GT que combine las dos propuestas en una o siga con las dos, los presidentes del GT, Mirja Kühlewind y David Black, están a favor de permitir que ambas sigan adelante. Mientras el IETF no puede decidirse por una ruta hacia una opción segura de TCP, Google está avanzando con una presentación individual de Quic como protocolo de transporte basado en UDP que también admite seguridad oportunista. El documento preliminar sobre Quic fue asignado a los administradores del Área de Transporte.

CFRG: ¿Se viene la criptografía post-cuántica?

El GT sobre Investigación sobre Criptografía está cerca de terminar su selección de nuevos algoritmos para TLS. En respuesta al pedido del GT sobre TLS, el grupo eligió dos nuevos algoritmos de curva elíptica: Ed25519 y Ed448. Todavía continúa la discusión sobre los hashes a utilizar para Ed448, porque existe la preocupación de que SHA3-512 no sea lo suficientemente eficaz. Sin embargo, el co-presidente Alexey Melnikov dijo que los hashes se elegirán a fin de año para completar esta ronda de selección de algoritmos. El pedido de nuevas curvas ha sido, en gran medida, una reacción a las revelaciones sobre Bullrun y otros programas similares de la Administración Nacional de Seguridad de los EE UU (NSA por sus siglas en inglés), que apuntan a debilitar la encriptación.

El Instituto Nacional de Ciencia y Tecnología de ese país (NIST por sus siglas en inglés), que había funcionado hasta ahora como fuente de nuevo material algorítmico para el cifrado, perdió su lugar como (casi único) proveedor de criptografía para el IETF por ahora. No se sabe aún si el CFRG, que se había centrado durante años en la investigación, se ocupará ahora de producir criptografía para los protocolos del IETF. No obstante, hubo un llamado a no utilizar criptografía que no hubiera pasado por una evaluación pública.

HELLO
PKCONF , pub-cipher-list, [cookie]
INIT 1 , sym-cipher-list, N C , K C , [cookie]
INIT 2 ,
sym-cipher, E NCRYPT (K C , N S)
Establecimiento de la conexión para la Opción TCP TLS:
SYN + TCP-TLS
SYN/ACK + TCP-TLS
ACK TLS Datos de solicitud de negociación (sobre TLS)".

Solo hubo algunas respuestas a la pregunta del co-presidente respecto de las próximas tareas del grupo. Se discutieron brevemente algunas ideas: la reducción de metadatos no encriptados (Bryan Ford), una posible estandarización del relleno (Stephen Farrell, de Trinity College) y criptografía post-cuántica (Ford, del Instituto Suizo de Tecnología, y Daniel Kahn Gillmor, de ACLU).

Recomendación de la NSA: ni se molesten en pasar a la criptografía de curva elíptica, por ahora

La recomendación de la NSA de esperar antes de pasar a la criptografía de curva elíptica si todavía no se ha hecho y, en cambio, esperar a que se desarrolle la criptografía post-cuántica (que estará disponible en breve) fue recibida con suspicacia por al menos parte de la comunidad, según Marcos Sanz (Denic). La declaración fue algo confusa, dijo el antiguo presidente del IETF y del IAB Russ Houseley (quien fue apoyado por la NSA durante su mandato). Esta reconoce claramente la posible necesidad de mitigar ataques, pero pide que, para ello, se pase a las claves largas en vez de a la criptografía de curva elíptica. Sin embargo, dadas las eficiencias de las curvas elípticas, muchas aplicaciones deberían cambiar.

El BoF sobre HOPS y la promoción de las mediciones en el IETF

Originalmente, el BoF sobre “Qué tan rota está la pila de protocolos” (HOPS por sus siglas en inglés) tenía por objeto trabajar sobre un nuevo protocolo de transporte que permitiera atravesar más fácilmente las áreas de la red cercadas por dispositivos intermedios. En lugar de atraer la inspección detallada de paquetes, el protocolo debía revelar algo de información sobre estos. Sin embargo, la idea de un protocolo "SPUD" (Protocolo sustrato para datagramas de usuario) no fue bien recibida, debido a que sus metadatos agregarían una capa más.

Ahora, los organizadores del BoF sobre HOPS proponen la creación de un Grupo de Investigación sobre HOPS dentro del IRTF. El nuevo Grupo de Investigación sobre HOPS (se espera que el nombre cambie) aspira a reunir académicos y operadores a fin de realizar estudios de medición y utilizar los resultados para el desarrollo de protocolos basados en los hechos. El grupo que se reunió en Yokohama, presidido por Brian Trammell y Mirja Kühlewind (los dos de ETH de Zürich), conversó largamente sobre la certeza de confidencialidad que se les daría a los operadores de la red para que abrieran las puertas de sus datos a los investigadores. Se trataron las Reglas de Chatham House e, incluso, las reuniones cerradas del grupo de investigación.

El presidente de la IAB, Andrew Sullivan, y el del IRTF, Lars Eggers, plantearon inquietudes (respectivamente, cómo podrían ayudar los datos no divulgados a persuadir a la gente a trabajar para la resolución de problemas, y el hecho de que un investigador podría tener que aceptar un acuerdo de no divulgación de datos de operadores de redes pero, de todos modos, podría presentar hallazgos anonimizados al grupo). Una representante del GSMA, Natasha Rooney, informó que esta organización está trabajando en la formalización de un proceso para recolectar datos y compartirlos con el grupo. Esto sería conveniente para los operadores, que se beneficiarían de los conocimientos especializados y de la elaboración de protocolos en el IETF. El GSMA y la IAB se reunieron durante la semana del foro (una reunión de seguimiento luego del Taller Marnew, que se presentó también en la reunión del SAAG, Grupo Asesor sobre el Área de Seguridad) para establecer una colaboración más estrecha.

Durante la reunión sobre HOPS, se realizaron presentaciones sobre proyectos de medición, como el de Infraestructura de Mediciones ARK de CAIDA, un observatorio de rutas con discapacidad y el uso de la colaboración abierta distribuida como recurso para realizar mediciones y para fundamentar el diseño de protocolos. Un grupo de la Universidad de Madrid utilizó la plataforma para colaboración abierta distribuida Microworkers con la finalidad de atraer usuarios (por pequeñas sumas de dinero) para que establecieran la conexión con el servidor que realizaba los experimentos acerca del estado de la encriptación de dichos usuarios.

Las mediciones, y el desarrollo de protocolos orientados por mediciones (o fundamentados por mediciones), fueron también el tema de la sección técnica de la plenaria combinada del IETF, la IAB y el IESG, que tuvo lugar el miércoles. Brian Trammell utilizó la pregunta "¿Internet puede funcionar sobre UDP?" como ejemplo para considerar la posible existencia de brechas a pesar de las muchas plataformas y herramientas de medición que ya están disponibles. El segundo presentador, Alberto Dainotti (CAIDA), urgió a que se recogieran más datos sobre el entorno del protocolo BGP, y anunció que se realizará una hackatón de mediciones sobre el BGP en vivo en febrero (contactar bgp-hackathon-info@caida.org). Durante la plenaria, hubo una reacción negativa considerable contra la demanda de más recolecciones de datos para alimentar las mediciones. En particular, se plantearon inquietudes respecto de posibles problemas de privacidad que resultarían del intento de medir datos cada vez más detallados sobre las redes.

Estandarización también para los usuarios, no solo para los grandes proveedores: el BoF sobre Estándares de Seguridad de la Información (ISS)

El único BoF en Yokohama fue impulsado por un grupo de académicos chinos de una antigua anfitriona del IETF, la Universidad de Tsinghua, que se enfrentó con un grupo ruidoso de los "superpoderes" de estandarización del IETF: Microsoft/Yahoo, Cisco y Google. Si bien se enfatizaron, en cierta medida, las ineficiencias de sincronización (de distinto grado entre distintos sistemas exclusivos), se señaló que el problema a abordar es la falta de interoperabilidad para los usuarios y la necesidad de que los desarrolladores se ocupen de las diferentes interfaces de programación de aplicaciones (API por sus siglas en inglés). El documento de planteamiento del problema afirma que "con la provisión de un protocolo de sincronización estándar, puede implementarse fácilmente un cliente tercero que admita múltiples servicios de almacenamiento de Internet, ya que los APIs ofrecidos por los distintos proveedores serían innecesarios o, al menos, se verían simplificados".

Durante el debate sobre el valor de la estandarización del IETF en esta área, las reacciones fueron bastante terminantes: no es de interés para los grandes monopolios del rubro, como Dropbox (400 millones de usuarios, 4 por ciento del tráfico). Un representante de Yahoo dijo que no se le ocurría ninguna razón para implementarlo. Sin implementación, el trabajo sería una pérdida de tiempo, afirmó Richard Barnes (Mozilla). Aun cuando el BoF terminó de manera poco optimista, hubo varios indicios de que podría ser interesante elaborar una norma para resolver problemas de la nube para usuarios individuales y ofrecer soluciones para empresas y/o para proveedores de almacenamiento en la nube de código abierto (https://syncthing.net/).

Después de la reunión del BoF, el presidente del IETF, Jari Arkko, reaccionó con una declaración en la lista de correos donde afirmaba que, aunque algunos proveedores grandes de espacio de almacenamiento pueden no estar interesados ("este espacio es grande") – entre ellos, nubes privadas, mercados empresariales, la Internet de las cosas, servicios de almacenamiento seguros – "también quisiera observar que los proveedores no son los únicos que especifican cuáles deberían

ser las soluciones. A menudo tenemos situaciones en las que los usuarios/clientes quieren estándares para incluir en sus solicitudes de ofertas (RFPs) de modo de crear un entorno más competitivo para los servicios que necesitan".

Cuando esta periodista les preguntó si les interesaría implementar un estándar, dijeron que con la actual proscripción de los servicios de Yahoo y Google en China, Baidu se hallaba en una situación demasiado cómoda. Si se permitiera la competencia, Baidu podría sentirse más inclinada a hacerlo.

Llamativamente, el BoF sobre ISS fue el único en Yokohama que generó una pregunta durante el periodo de micrófono abierto de la sesión plenaria. El liderazgo del IETF indicó las nuevas tareas en marcha: tres nuevos GTs están por ser aprobados por el IESG.

Grupo de investigación sobre derechos humanos

Luego de dos sesiones consecutivas de BoFs y otra del IRTF, la constitución de un Grupo de Investigación del IRTF sobre derechos humanos es inminente (el acta constitutiva se encuentra aquí). Los co-presidentes, Nils ten Oever y Avri Doria, presentaron un videoclip que compila extractos de entrevistas realizadas dentro de la comunidad del IETF que muestran que el tema se ha convertido (casi) en una cuestión corriente. El clip muestra a los líderes del IETF, incluyendo a su presidente, Jari Arkko, y a Scott Bradner, miembro de la Junta – así como a muchos desarrolladores de la comunidad del DNS, entre ellos, el presidente de la IAB, Andrew Sullivan, y el investigador de la AFNIC Stéphane Bortzmeyer – reflexionando sobre la relación entre los derechos humanos y la estandarización. Como afirmó Arkko, los protocolos técnicos siempre pueden tomar uno u otro camino.

Si bien todavía existe algo de preocupación en el grupo del IRTF/IETF acerca de la falta de definición del alcance del grupo de investigación sobre derechos humanos, uno de los primeros documentos preliminares presentados en Yokohama fue un documento preliminar informativo que exhorta a que la elaboración de protocolos tenga por objeto, en primer lugar, servir al usuario. El documento preliminar del presidente del GT sobre HTTP2, Mark Nottingham, podría ser visto claramente como una reacción al pedido de Edward Snowden a los desarrolladores que ayuden a los usuarios brindando mejor seguridad y control de su comunicación.

El llamado a prestar atención, en primer lugar, a los intereses de los usuarios sería un cambio respecto de la percepción actual del IETF acerca de su propia tarea, ya que se ocupa, ante todo, de los problemas de los operadores y proveedores. Según Andrew Sullivan, presidente de la IAB, no queda claro quiénes son los usuarios. Esta también es una pregunta difícil de responder en el caso de la comunicación entre máquinas.

La próxima reunión del IETF se realizará del 3 al 8 de abril de 2016 en Buenos Aires