Informe de CENTR
IETF99
Praga, 17-21 de julio de 2017

Traducción - LACTLD

LACTLD agradece a Hugo Salgado (nic.cl), por la revisión de la Edición en Español

Para acceder a la versión en inglés de este informe ira a Highlights de: **https://centr.org/**

Aspectos destacados

El IETF y las políticas de los estándares

El debate sobre la naturaleza política de los estándares y potenciales éticos en la estandarización ha cobrado visibilidad en los debates del IETF gracias a Snowden. Si bien la asistencia al dedicado grupo de trabajo del IRTF, sobre las Consideraciones de los Derechos Humanos en los Protocolos (HPRC), se ve limitada a un número de desarrolladores altamente interesados, las preocupaciones sobre la privacidad en los diseños se reflejan cada vez más en varios otros grupos de trabajo (WG).

En línea con la presentación de Dave Clark sobre la "lucha" —el dilema entre los derechos e intereses contrapuestos en el desarrollo tecnológico (vea el Informe de CENTR IETF98)— el Presidente del WG de HPRC, Niels Ten Oever, y el expresidente del IAB y reconocido experto en DNS (antes en Dyn y ahora en Oracle), Andrew Sullivan, se reunieron para aclarar la relación entre las políticas y los estándares, y elaboraron las ideas en un nuevo documento RFC draft. Presentado en la reunión de Praga, el documento explora las diferentes concepciones de las políticas/estándares o la relación de la estandarización en un espectro de posiciones que van desde "la tecnología es neutral" a "los estándares son políticas que utilizan otros medios".

Con respecto al propósito del documento, los autores y defensores lo consideraron como un posible curso intensivo de "políticas y estándares" para la comunidad del IETF, que puede alejarse de la original "Investigación sobre las Consideraciones de los Derechos Humanos en los Protocolos", que se encuentra camino a la elaboración del draft de la primera RFC del WG de HPRC.

"El código no es la ley"

Milton Mueller (Georgia Tech), reconocido profesor de políticas de tecnología, cuestionó la idea de que los desarrolladores de estándares y tecnólogos pudieran ejercer una influencia significativa sobre las reglas de comunicación en la Internet. A lo sumo, la tecnología posee una función de mediación para los derechos humanos (DD. HH.). Mueller rechazó el argumento de Lessig en el que afirmaba que el código es la ley. "El código no es la ley", expresó, y agregó que la ley usualmente "sobrescribe" las opciones tecnológicas. Mueller señaló el desarrollo de la legislación sobre escuchas telefónicas de Ley de Asistencia de las Comunicaciones para la Aplicación de la Ley (CALEA, por sus siglas en inglés) en contra de la negación del IETF (en la RFC 2804) como ejemplo principal. A fin de cuentas, la protección de los DD. HH. representaba un esfuerzo institucional y político, pero no tecnológico.

Entonces, aunque es bueno que los desarrolladores "sean conscientes" de estos problemas, su influencia se ve limitada. Junto con Farzaneh Badii, Mueller se encuentra elaborando un documento que cuestiona la idea de "promover los derechos mediante la arquitectura de Internet". Mueller y Farzaneh hablan de un "Réquiem por un sueño".

Algunos argumentos extra de Mueller en relación con la necesidad de "despertar" de ese sueño fueron que: la evaluación de los derechos era solo posible de manera *ex-post* (en lugar de ser descifrados de manera *ex-ante*); el diseño de Internet era ya demasiado estable para realizar grandes cambios en él; y los DD. HH. eran complejos e incluyen el equilibrio de intereses contrapuestos. Al mismo tiempo, Mueller advirtió sobre la tentación de tomar decisiones sin obtener las opiniones de otras partes interesadas. La politización de los estándares podría así resultar en el cuestionamiento de la legitimidad de los desarrolladores técnicos para el diseño y podría también llevar a otros grupos, especialmente legisladores y gobiernos, hacia el proceso de estandarización.

Claramente, Ten Oever refutó esto último, señalando que los gobiernos participan hace ya mucho tiempo en el proceso de estandarización, incluso en el IETF. El NIST y la NSA, por ejemplo, participan habitualmente y, con los años, mediante su propio personal o representantes patrocinados, han desempeñado papeles principales en el IETF/IRTF. Tanto Georg Mayer (Presidente de CT del 3GPP) de Huawei como Bob Hinden hicieron énfasis en los cambios significativos que se realizaron y realizarán en las redes móviles y el cifrado. El potencial para deshabilitar o habilitar a monopolios mediante estándares podría también tener un efecto en los DD. HH., según señaló Philip Hallam-Baker (Commodo). Finalmente, Allison Mankin, Presidente del IRTF, apuntó a los debates sobre la posibilidad de regular los algoritmos (antes de que sean ellos quienes nos regulen).

Los estándares y las políticas en la práctica

La política está muy arraigada en la toma de decisiones para los diseños de los estándares involucrados, como se puedo ver claramente durante la reunión IETF99.

En tres WG diferentes, se generaron debates apasionados sobre los requisitos presentados por operadoras que, según expertos en privacidad y seguridad, no lograron alcanzar los estándares del IETF en relación con las comunicaciones seguras y respetuosas de la privacidad. Estos requisitos fueron: (1) contar con un nuevo registro de recursos XPF en el WG del DNS que empaquete la información personalmente identificable en paquetes del DNS (PII) para ayudar al balanceo de carga; (2) revelar información sobre la duración de los viajes de ida y vuelta en el nuevo protocolo de transporte Quic para la gestión del tráfico; e (3) incluir la posibilidad de utilizar una Clave Diffie-Hellman estática en el nuevo estándar TLS 1.3 para poder ver el tráfico directamente "en el cable" (on the wire) desde y hacia los datacenters, para la resolución de problemas.

Jamás se había percibido tal tensión en una reunión IETF sobre una sola cuestión —el conflicto de intereses entre la privacidad/seguridad y los intereses operacionales de las compañías—, según observó Sara Dickinson, experta en el DNS y la privacidad del DNS, en Sinodun. En los resúmenes sobre el DNS, el TLS y el WG de Quic que se muestran a continuación, se puede leer una breve recapitulación de estos debates.

¿Un registro XPF en el DNS? ¿En serio?

Añadir información personalmente identificable sobre los clientes del DNS —sin que ellos lo sepan— es una práctica que ya llevan a cabo varios proveedores de DNS, y algunos vendedores ya la tienen disponible en la maquinaria DNS, activable opcionalmente. Durante la segunda de las dos sesiones del WG del DNS (vea más abajo), se presentaron dos propuestas que supuestamente abordan los problemas dela administración de red del DNS. Se debatieron las cuestiones "Un identificador de cliente en consultas DNS reenviadas" y el nuevo registro de recursos DNS X-Proxied-For (XPF).

En "Un identificador de cliente", los autores (incluido David Lawrence, Akamai) subrayaron la necesidad de permitir "repuestas del DNS personalizadas", como por ejemplo "control parental". Para XPF, elaborado por autores del ISC y PowerDNS, el razonamiento es el uso de dispositivos proxy y la negativa de direcciones de origen oculto para el balanceo de carga.

Mientras que XPF tiene la intención de ubicarse entre el balanceador de carga y el servidor real y debería, en teoría, quedarse en las instalaciones del servidor, la Conexión ID se ubicaría entre la máquina del usuario final y un proveedor. Este último podría considerarse mucho más riesgoso, según expresó Stéphane Bortzmeyer, experto en el DNS, de Afnic. No obstante, ambas propuestas van en la misma dirección: ambas añaden metadatos en las consultas del DNS y habilitan el monitoreo generalizado.

El debate sobre estos drafts ciertamente aclara que añadir información personalmente identificable desde direcciones IP hasta direcciones MAC o, como propone el draft del ID de Cliente, "otros valores definidos de tipo identificador", es una práctica común para algunas operadoras, incluidas las compañías como Cisco, Nominum o PowerDNS. Por lo tanto, querrían que se apruebe un documento de estándares —o aunque sea un documento informativo que lleve el sello del IETF. Sin embargo, muchos participantes en la comunidad ccTLD del DNS y expertos en privacidad están preocupados debido a que esto irá en contra de los esfuerzos para hacer que el DNS sea más respetuoso de la privacidad y cumpla con la legislación sobre privacidad.

La lucha del equilibrio entre la facilidad de uso de los operadores y una mejor protección de la privacidad no se bate exclusivamente en la comunidad del DNS. Parece ser una tendencia común en el IETF estos días, con el WG del TLS y el de Quic en constantes duelos sobre dichas posiciones en extensas discusiones durante las sesiones en Praga.

El progreso de Quic y cuánta información debería quedar expuesta en línea

Para muchos, Quic es uno de los progresos más importantes del IETF, ya que es el primer intento en la creación de un sucesor para el TCP hace ya algún tiempo. Según las cifras presentadas por

Jana Iyengar (Google) durante el Grupo de Investigación de Evaluación y Análisis de Protocolos (MAPRG, por sus siglas en inglés), el 35 por ciento de todo el tráfico de la web y el 7 por ciento de todo el tráfico de Internet viaja a través de Quic actualmente.

Al utilizar el UDP como sustrato, Quic representa un protocolo de transporte con cifrado inmediato (objetivo: TLS 1.3, y 0RTT en conexiones restablecidas) y también promete deshacerse del "bloqueo del primero de la fila" ("*head of line blocking)* del TCP mediante el uso de flujos múltiples (*multistreams*) y números de paquete con incremento estricto.

Código de funcionamiento: Primera Interop con Google, Mozilla y otros

El WG de Quic se reunió en una primera Interop (prueba de interoperabilidad) poco antes del IETF99 para probar cinco implementaciones del nuevo protocolo de transporte que Google presentó al organismo de estandarización tras probarlo por varios años en sus redes.

En la reunión Interop, se presentaron cuatro implementaciones más además de las de Google: Mozilla, una implementación Microsoft de Christian Huitema, una implementación de WireShark y otra pequeña del copresidente del WG de Quic, Lars Eggert. En resumen, lograron una negociación (*handshake*) para establecer una conexión Quic básica y un cierre. En la primera de dos sesiones del WG, se originó un debate sobre cuán ambiciosa debía ser la segunda Interop, en el que Mozilla y Google urgieron incluir al menos una pequeña aplicación, o incluso flujos paralelos o multiplexados.

Iyegar instó llegar a un acuerdo sobre la codificación en la red de los paquetes de Quic tan pronto como fuera posible para evitar que los *middleboxes* se amarren al Quic de Google, generando problemas de implementación para el Quic del IETF, que efectivamente se ve diferente en el cable. El formato del encabezado fue un aspecto de Quic que sufrió cambios durante el primer año de trabajo del WG de Quic. Los indicadores que Google había incluido en los encabezados de Quic, por ejemplo, fueron eliminados. Aun así, estos mismos indicadores, según Iyengar, sirven para que los *middleboxes* detecten a Quic.

Actualmente, una de las cuestiones que se debaten con respecto a Quic es el mapeo de http sobre Quic. Hay quienes advierten también no concentrarse solamente en el mapeo de http, sino en hacer que Quic sea un verdadero protocolo genérico. Otro debate en curso tiene que ver con los flujos unidireccionales o bidireccionales. Sin embargo, el problema más controvertido en este momento son, como se menciona anteriormente, las consideraciones con respecto a la privacidad.

¿Cuánto invaden la privacidad las medidas RTT pasivas?

Los avances en el cifrado de transporte con TLS prácticamente incorporado en Quic son bienvenidos debido a razones de seguridad y privacidad (y su eficiente provisión). Una causa de preocupación para los operadores de redes es el paso en el que también se cifran partes del

encabezado y solo se dejan unos pocos elementos en la parte visible de este, específicamente un número de *Tipo* (5), *Versión* (32) y Número de *Paquete* (8/16/32), con una *Conexión ID* opcional. Perderán información filtrada de los encabezados TCP que es usada para la gestión de la red y resolución de problemas, en específico la gestión de las filas y la congestión.
En un debate similar al del WG del TLS y el del DNS, los operadores hicieron fila en el WG de Quic para solicitar un mecanismo que les devolviera algo de su habilidad para medir los Tiempos de Ida y Vuelta (RTT).

Para tomar una decisión, Ian Swett (Google) presentó cuatro opciones sobre cómo proceder: (1) dejarlo todo como está; (2) eco del número de paquete; (3) un spin bit configurado por RTT; o (4) un valor de bit idéntico para un RTT de paquetes. Tras evaluar las ventajas y desventajas de mantener el statu quo, que sólo hace que el *handshake* del RTT sea visible, pero nada más, Swett reconoció que las operadoras de redes y *middleboxes* innovadores podrían "intentar inferir el RTT" o recurrir a otras técnicas, o incluso bloquear los paquetes de Quic. Varias operadoras, al igual que Brian Trammell (ETH Zurich), lo confirmaron.

2. Eco del Número de paquete: "El paquete enviado expone un número de paquete y el otro lado hace eco de ese número de paquete sólo sobre paquetes ACK"

3. Idea del spin bit: "Un paquete por viaje de ida y vuelta establece un spin bit en el encabezado hacia arriba (1) y otros son enviados con el bit hacia abajo (0), el cual debe hacerse eco en el otro lado".

3a. Bit idéntico: "El iniciador de la conexión envía paquetes con un valor de spin hacia arriba, el par refleja el spin en paquetes de respuesta, y el iniciador da vuelta el spin".

Las opciones 2, 3 y 3a fueron rechazadas, ya que no debería estar permitido rehabilitar el monitoreo pasivo y la vigilancia, especialmente debido a los posibles abusos en el futuro, independientemente de las justificaciones actuales. Iyengar expresó que al menos Quic ya resolvería los problemas actualmente abordados por la gestión de las filas mediante el comportamiento avanzado de Quic con respecto al multiplexado y el facilitamiento de los flujos de tráfico.

Luego de 90 minutos durante los cuales ninguna de las partes dio brazo a torcer, se acordó un grupo de diseño presidido por Ted Hardie (Google). El grupo intentará evaluar los efectos de prohibir que los encabezados de Quic pongan a disposición cierta información y, por otro lado, los efectos en la privacidad de ceder ante la solicitud de los gerentes de redes.

Quic mantendrá otra reunión entre sesiones previa a la reunión IETF100 en Seattle, que tendrá lugar en octubre. La reunión entre sesiones contará con una reunión Interop y varios días de reuniones habituales de los WG. Según Lars Eggert, cerca de 60 personas asisten a estas reuniones entre sesiones.

La lucha sobre una clave de custodia en datacenters para TLS

El Grupo de Trabajo de la Seguridad de la Capa de Transporte (WG de TLS) está a punto de finalizar la versión TLS 1.3, el estándar sucesor de TLS 1.2. Las características más importantes incluyen: el secreto hacia adelante obligatorio ("forward secrecy"), el establecimiento de una conexión cifrada de una ida y vuelta, y la habilidad de evitar ataques de baja de versiones (*downgrade attacks*) (de la versión 1.3 a la 1.2). Tras una segunda RFC de última llamada del WG, el autor Eric Rescorla (Mozilla) solicitó unas semanas más para probar el nuevo estándar luego de que las primeras rondas de prueba (en Mozilla, Google, y, sin haber aportado datos trasparentes, Facebook) revelaron un aumento en las tasas de errores.

Las tasas de errores arrojadas iban de 1 a 10 por ciento, según Rescorla. En Google, según una fuente, el establecimiento de la conexión con TLS 1.3 falló en el 5 por ciento de los casos.
Martin Thomson (Mozilla) dijo que se creía que el problema eran los *middleboxes* de dos (importantes) compañías. Es por esto por lo que los desarrolladores quieren continuar con la etapa de prueba. Probablemente, esto resulte en otro retoque en el texto draft del estándar. Una solución básica en consideración es cambiar el tipo de contenido del "Server Hello". El WG tendría que llegar a una decisión consensuada final con respecto a ese retoque. No se reveló cuáles fueron las compañías en cuestión.

Husmeando todo el tráfico en el datacenter

El tema delicado en TLS, sin embargo, no tiene que ver con las modificaciones extra de la especificación para poder introducir los paquetes cifrados de TLS 1.3 mediante *middleboxes.* Se trata, en cambio, de cuánto se debe modificar el nuevo TLS para permitir que las operadoras de redes controlen el tráfico en sus datacenters. Una propuesta para el uso de una clave Diffie-Hellman estática que permita tener una llave de custodia ("escrow key") en el datacenter disparó una batalla épica en el WG de TLS. Si esto se incorpora en la RFC propuesta para el estándar, se rompería la seguridad hacia adelante de TLS, lo que permitiría que las operadoras husmeen todos los datos que circulan desde y hacia sus servidores.

En resumen, la propuesta busca que sea una opción contar con una clave estática (que se rote frecuentemente), en lugar de las claves efímeras que son obligatorias según la especificación del draft del estándar propuesto para TLS 1.3.

La propuesta fue elaborada por Matthew Green, reconocido experto en seguridad, quien había sido contratado por varias compañías pertenecientes a la industria bancaria (y a la industria de la seguridad de la red). Otros autores incluyen al expresidente del IETF, Russ Housley (VigilSecurity), y al exdirector de área de Internet del IETF, Ralph Droms. Hasta el momento, los autores incorporan únicamente compañías de EE. UU. que han recibido el apoyo de NIST, la agencia estadounidense de tecnología de seguridad informática y de red. La agencia NIST había reunido al grupo de la industria en un taller para formular su propuesta y anunciar también en la reunión del IETF en Praga que presentaría una propuesta propia para resolver el problema del monitoreo.

“Es espionaje”, vociferó Stephen Farrell, exdirector del área de seguridad, quien recopiló una larga lista de argumentos contra el hecho de que el IETF siquiera siga debatiendo la propuesta.

El murmullo final reveló que los participantes estaban divididos en casi un 50-50.

Se espera que el debate sobre las puertas traseras de TLS continúe, a pesar de que algunos opositores declararon que este problema “murió” tras el debate en Praga. Por otro lado, durante una conversación luego de la sesión, los miembros del grupo de los defensores también cantaron “victoria”, ya que esperaban que el WG se pronunciara más claramente en contra de la opción de la clave de puertas traseras.

Un ramillete de nuevas opciones de Transporte del DNS: ¿cómo elegir?

DNS sobre TLS, DNS sobre Http, y DNS sobre el nuevo Quic: todos fueron presentados en la reunión de Praga. Algunos espectadores como Alex Mayrhofer alertaron contra forzar el nuevo competidor de transporte “Quic” a expensas del DNS sobre TLS. La preocupación es que la competencia podría resultar en crear incluso más dudas a los implementadores con respecto a poner en práctica el DNS con mejoras en la privacidad en el DNS sobre TLS.

Sara Dickinson (Sinodun) matizó la preocupación. Al ser al mismo tiempo una de los desarrolladoras de un paquete de software de resolutor *stub* del DNS sobre TLS y autora del draft aún en bruto “DNS sobre Quic” (junto con Christian Huitema, Microsoft), expresó a quien escribe que Quic podría representar una solución muy interesante para la parte del camino desde el resolutor al servidor autoritativo, por razones puramente relacionadas con la eficiencia. A mediano plazo, todavía era necesario implementar el DNS sobre TLS. También pensó que hacer el esfuerzo de implementar el DNS sobre TLS primero fue beneficioso para aquellos que luego recurrirían a Quic, ya que el esfuerzo de cambiar a Quic con cifrado incorporado sería mucho más llevadero. Fue, desde luego, el primer paso hacia la concientización sobre el DNS como un servicio prudente en cuanto a la privacidad.

En un breve comentario hacia la autora, Erik Kline de Google expresó una idea similar: “estamos en el proceso de hacer primero que el DNS sobre TLS funcione y se integre. Todos estos transportes alternativos requerirán más trabajo (y forzosamente reutilizarán mucha de la integración de TLS, así que tiene sentido que primero probemos el TLS). [...] Puede suceder que la experiencia operativa con el DNS sobre TLS informe cómo progresan los transportes alternativos. Probablemente necesitarán realizarse algunas medidas para comparar la capacidad de alcance en el puerto 853 con el puerto 443, para empezar”.

Pasos de implementación del DNS sobre TLS

En la actualidad, existen 12 resolutores recursivos que aceptan las consultas cifradas de TLS, siendo un nuevo servidor en el *Korean Internet Exchange*, KINX, la última incorporación. El IETF también

llevó a cabo un experimento para el DNS sobre TLS durante la reunión del IETF. Su adopción aún es lenta (tanto que Stéphane Bortzmeyer, de Afnic, aseguró haber dudado impulsar la continuación del trabajo con respecto a los documentos de privacidad de recursivos a resolutores). Sin embargo, un representante de Dyn mencionó durante la reunión en Praga que al menos él había tenido la intención de trabajar también en la implementación. El trabajo de implementación del Hackathon se puede ver aquí.

Software del DNS sobre TLS

Fundado por la NLnet, el proyecto de privacidad del DNS continúa monitoreando la implementación en los paquetes de software para los resolutores recursivos: vea la descripción general en dnsprivacy.org. Tanto Unbound como Knot reúnen la mayoría de las características. Ondřej Surý confirmó que atender las solicitudes del TLS hacia arriba desde el resolutor estaba en la lista de pendientes, para que Knot reúna otra característica. Por el momento, para BIND, se necesita un stunnel proxy para implementar el DNS sobre TLS.

Del lado del *Stub*, se avanzan los trabajos en Stubby por parte de Sinodun con paquetes trabajados en Mac, Microsoft y Linux. Está en marcha el desarrollo de una interfaz gráfica (GUI) que sea fácil de usar (que permitirá convertir el DNS sobre TLS en la *laptop*, o en la computadora de escritorio). Estará disponible cerca de la fecha del próximo encuentro del IETF. Por el momento, no se planifica desarrollar un GUI para Linux, debido a restricciones en los costos y la idea de que los usuarios de Linux serían geeks y usarían la línea de comandos de la versión de Stubby.

También se presentó la implementación del DNS sobre TLS en Android durante el Hackaton en Praga. Ben Schwartz de la oficina de Nueva York de Google realizó una demostración del funcionamiento del DNS sobre TLS en un Android construido a medida durante Bits-n-Bytes. El trabajo del DNS sobre TLS se está llevando a cabo en AOSP (Teclado Android).

Pese a estos pasos, la implementación continúa siendo lenta y los expertos describen los sucesos como una situación “huevo-gallina” en la que grandes implementadores como Google (que ya utiliza DNS sobre HTTP) esperan más demanda por parte de los usuarios, mientras que estos esperan la intervención de los grandes proveedores de DNS. En respuesta a un pedido realizado por quien escribe, Lennard Poettering, Red Hat y el principal desarrollador de software de Linux, explicó que systemd-resolved no pretendía tomar la delantera en el desarrollo del DNS, sino que buscaba una buena implementación para clientes de las tecnologías exitosas del DNS. El DNS/TLS no había llegado a esa instancia todavía, debido a que no había suficientes implementaciones. “Si los DNS/TLS se implementan de manera generalizada, podemos apoyar la implementación directamente mediante systemd-resolved”. Aunque la seguridad tomó un papel principal y DNSSEC, por ejemplo, se había implementado, el DNS sobre TLS no estaba listo todavía. Como respuesta a qué representaba un éxito, Poettering brindó los siguientes ejemplos: si Google lo usara para sus servidores DNS públicos, si Deutsche Telekom lo utilizara en el servidor DNS para T-DSL, si el DNS Proxy de FritzBox lo utilizara, o si lo usara el servidor Red-Hat para una VPN.

DNS sobre HTTP2

El DNS sobre HTTPS es una idea alimentada por la “gente de los navegadores”. El objetivo es hacer que el DNS esté más completamente disponible para las aplicaciones. Paul Hoffman (ICANN) dijo que la motivación detrás del DNS sobre HTTPS es que “los navegadores web pueden solamente lidiar con las direcciones IP fácilmente, las aplicaciones solo pueden lidiar con las direcciones IP”. Las aplicaciones basadas en la web que quieren usar funciones del DNS, como DANE, el descubrimiento de servicios DNSSD, actualmente deben utilizar extensiones en el navegador. Al mismo tiempo, el DNS sobre HTTP2 representó el mecanismo más práctico para una comunicación de extremo a extremo confiable. El TLS brindó integridad y confidencialidad, y el HTTP facilitó el tránsito a través de proxies, cortaafuegos y sistemas de autenticación. Hoffman y Patrick McManus (Mozilla) proponen usar “GET” o “POST” para envolver las consultas del DNS (ya sea en el mensaje o en el cuerpo). Utilizar el método GET es más amigable con muchos cachés HTTP y es más pequeño.

El draft señala que:

Una consulta para los registros IN A para “www.example.com” con la recursión activada utilizando el método GET y una solicitud de codificación en la red sería:

:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /.well-known/dns-query? (Sin CR)
content-type=application/dns-udpwireformat& (sin CR)
body=q80BAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-udpwireformat, application/simpledns+json

La misma consulta de DNS, utilizando el método POST sería:

:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /.well-known/dns-query
accept = application/dns-udpwireformat, application/simpledns+json
content-type = application/dns-udpwireformat
content-length = 33

<33 bytes representados por los siguientes códigos Hex>
abcd 0100 0001 0000 0000 0000 0377 7777
0765 7861 6d70 6c65 0363 6f6d 0000 0100 01

Este draft no es el primero en abordar el DNS sobre HTTP, vea propuestas anteriores elaboradas por Hoffman. Las versiones más antiguas usan http en lugar de https. Ahora el http (http2) debería ser la primera opción. A pesar de que Hoffman criticó abiertamente el desarrollo del DNS sobre Quic, advirtiendo sobre su posible confusión con respecto a la implementación del DNS sobre TLS, dijo que el DNS sobre HTTPS era una solución para que la gente de los navegadores y las aplicaciones usen el DNS de una manera más integral y segura. Se asumía también que el DNS sobre HTTPS podría ser implementado rápidamente por alguien que estuviera a cargo de un gran servicio web sin mayores esfuerzos para hacer funcionar un resolutor recursivo sobre su http2.

El interés en Google está documentado mediante la implementación de Google del DNS sobre HTTPS.
Por otro lado, la privacidad no fue la preocupación principal, incluso si el caso fuera que el DNS sobre https lograra implementarse, "todo el tráfico web sería privado". Hoffman rechazó la propuesta de los presidentes del WG de DISPATCH de enviar el draft a la Privacidad del DNS.
Con respecto a la inquietud sobre que más información terminaría en el datacenter del proveedor del navegador, Hoffman dijo que de todos modos, hoy en día, las personas no estaban escogiendo su resolutor recursivo, y que, en cambio, utilizaban servicios como el de Gooogle.

DNS sobre Quic

El DNS sobre Quic es la alternativa más novedosa para el transporte del DNS. Durante el WG de DPRIVE, Christian Huitema introdujo su argumento a favor: combinará el DNS sobre TLS como funciones de cifrado con ventajas para el transporte, especialmente permitiendo el reestablecimiento de la conexión 0RTT y la eliminación del "bloqueo del primero de la fila" ("*head of line blocking")*.

Debido a que el WG de Quic actualmente está trabajando en las especificaciones base —y el transporte http fue tomado como un hito para el WG—, se rechazó la incorporación de otros protocolos a la agenda de Quic durante la sesión del WG de Quic. Huitema argumentó que Quic no debería estar especificado perdiendo de vista a los otros "consumidores de transporte".

Durante el WG de DPRIVE, una de las inquietudes más importantes con respecto al draft propuesto fue que estaba orientado hacia el camino del resolutor *stub* al resolutor recursivo únicamente. Para el transporte de Quic, esta división no debió repetirse y, quizás, no haya sido necesaria, según dijo Andrew Sullivan. Las ofertas paralelas de diferentes variantes de transporte del DNS podrían también confundir a los implementadores.

Sedes: El IETF cambia la sede de la reunión para evitar EE. UU.

Apenas un día antes del comienzo de la reunión del IETF en Praga, el IAOC publicó su decisión sobre cambiar la sede de la reunión en julio de 2018 para evitar posibles problemas migratorios en EE. UU. Habiendo escogido San Francisco como la sede para el IETF102, el IAOC debió cancelar el

contrato con el hotel de conferencias y negociar uno nuevo, pero podrá recuperar la tarifa de la cancelación al momento de regresar al hotel de San Francisco para mantener una reunión durante los próximos años. La reunión ahora tendrá lugar en Montreal, Canadá, una semana después de la reunión que se había planificado en San Francisco.

La razón de esta decisión del IAOC fue la situación migratoria poco clara de EE. UU. tras los cambios en las políticas fronterizas estadounidenses y las posteriores decisiones de la Corte. Esto dio como resultado un "ambiente de incertidumbre", así que el IAOC decidió ir a lo seguro y cambiar la sede. Los resultados de una encuesta también arrojaron que el 15 por ciento de los 211 encuestados había decidido no viajar a la reunión de Chicago en marzo de 2017.

Curiosamente, Praga fue elegida una vez más como la sede europea para la reunión de 2019. En cuanto a las reuniones en América del Norte, Canadá podría convertirse en la sede principal, como lo ha sido por varios años en este último tiempo.

Políticas de selección de sede para las reuniones

Como conclusión del debate sobre las sedes de la reunión, se preparó un documento draft para regular la futura selección de sedes. El debate se originó a partir de una queja del presidente del IAB, Ted Hardie, sobre la elección de Singapur como sede para el IETF100 a pesar de la legislación vigente anti-LGBT, pero también fue influenciado por los debates sobre los sobresaltos en las políticas migratorias estadounidenses.

El draft Sede de la Reunión incluye el objetivo declarado "de minimizar las situaciones en las que regulaciones migratorias onerosas dificultan, desmotivan o impiden que los participantes asistan a las reuniones. En caso contrario, distribuir los sitios de las reuniones de manera que dichas regulaciones no siempre afecten a los mismos participantes". El documento también urge evitar reuniones en países con "leyes que en la práctica excluyen a personas por motivos de etnia, religión, género, orientación sexual, nacionalidad, o identidad de género".

El draft de la RFC incorpora criterios para la selección de la sede y del hotel y un proceso paso a paso para llevar a cabo la selección. También se especificó que debe haber una publicación anticipada de las posibles sedes para la reunión y un espacio para los comentarios de la comunidad, para mejorar la transparencia y la participación en el proceso. El documento sigue en discusión.

Se propusieron roles en el proceso de selección para:

1. El Comité de Supervisión Administrativa del IETF, el IAOC, (supervisar y seleccionar las sedes para las reuniones del IETF, instruir al IAD que trabaje conjuntamente con la ISOC para redactar contratos, asegurando que se evalúen las inquietudes de los participantes acerca de la sede);

2. La Actividad de Apoyo Administrativo del IETF, la IASA, (llevar a cabo el proceso de selección de la sede bajo la supervisión del IAOC);

3. La Secretaría del IETF (parte de la IASA bajo la gestión del IAD);

4. El director administrativo del IETF (coordinar y apoyar las actividades de la Secretaría del IETF, del Comité de Reuniones del IAOC y del IAOC, gestionar el presupuesto para las reuniones); y,

5. El Comité de Reuniones del IAOC (participar en el proceso de selección de la sede, hacer un seguimiento del programa de patrocinadores de la reunión).

IASA 2.0

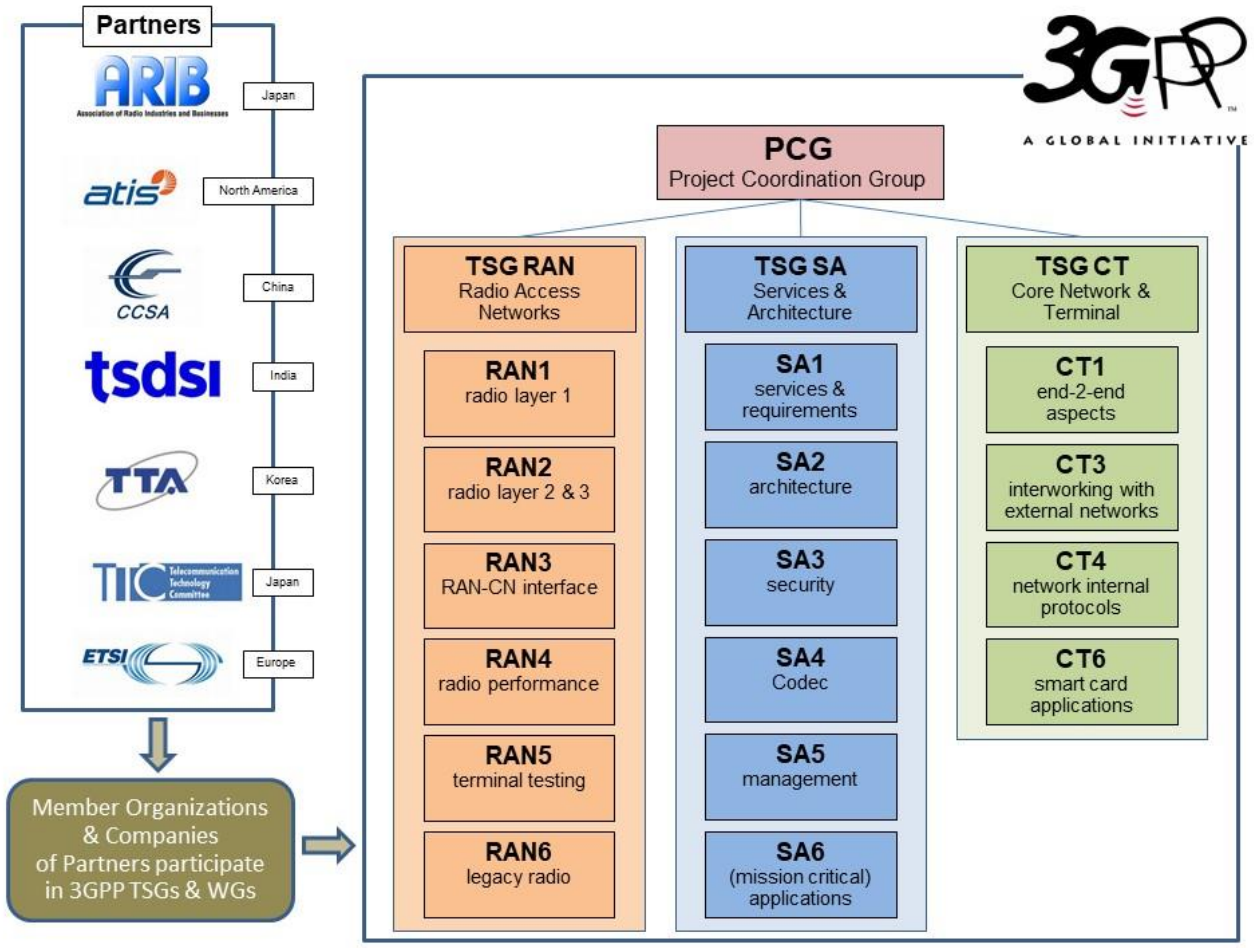
Aunque los roles en el proceso de selección de la sede están bien delimitados, la propia estructura de la IASA está atravesando un debate en el que un equipo de diseño habla sobre cómo se podría reestructurar la administración del IETF. Con estos debates de reestructuración en curso, no habrá un remplazo inmediato para Ray Pelletier, primer y antiguo IAD (y persona a cargo de preparar la selección de la sede de las reuniones). Pelletier dejará su cargo antes de la reunión en Singapur.

Las tres opciones para la futura administración que presentó el equipo de diseño en Praga fueron: (1) IASA PlusPlus (modificaciones menores, la estructura se conserva); (2) una subsidiaria de la ISOC; o (3) una organización independiente.

Grupos de trabajo (WG) y grupos de debate informal (BoF)

BoF sobre NetSlicing y el 3GPP

Durante un almuerzo de trabajo y un BoF sobre NetSlicing, el IETF y el organismo móvil de estandarización 3GPP intentaron alinear mejor su trabajo, especialmente a los efectos del actual proceso de estandarización 5G. Debido a que el 3GPP está reutilizando muchos protocolos del IETF, Georg Mayer, presidente de Red de Núcleo y Terminales del 3GPP (para conocer la estructura del 3GPP, vea el gráfico más abajo), instó a que el IETF presentara rápidamente cualquier cuestión que los desarrolladores del IETF consideraran que deberían estar incorporadas en las especificaciones base del núcleo del 5G. Sin embargo, el 3GPP todavía debe tomar una decisión con respecto a qué protocolos del IETF utilizará: Diamater, HTTP1, HTTP2, o incluso Quic (aunque Mayer aclaró que podría ser demasiado tarde para Quic). En cualquier caso, las especificaciones base (versión 15 del documento sobre el 5G) debían estar listas para junio de 2018. El calendario también está establecido debido a las preparaciones para la próxima Conferencia Mundial de Radiocomunicaciones de la UIT en 2019, momento en el que se deberán defender los casos de uso para la siguiente ronda de asignación de frecuencias.



El "rebanado" de la red (*Network Slicing*)

En el 3GPP, el rebanado de la red es un concepto principal para que el 5G exprese la idea de que, en lugar de una sola red en el futuro, se espera que la red esté dividida para diferentes usuarios y casos de uso, lo que también permite una diferente calidad del tráfico. Este concepto surgió como reacción a la diferenciación de clientes: en lugar tener sólo operadoras de telecomunicaciones y sus clientes, ahora existían operadores de redes de sensores, la industria automotriz o los usuarios de drones o arquitectos de ciudades inteligentes, cada uno con su conjunto de requerimientos específico para su conexión de redes. En lugar de una red que sirva para todos, se podrían ofrecer estas "rebanadas" a dichos clientes.

El BoF sobre el rebanado de la red reveló, más que nada, que los conceptos que tenían el 3GPP y el IETF sobre el rebanado de la red eran enormemente diferentes. Ted Hardie, presidente del IAB, señaló que era necesario que ambas organizaciones llegaran a un acuerdo sobre la definición del rebanado, así como también de otros términos. El próximo paso en el esfuerzo de mejorar la cooperación podría ser la elaboración de un draft sobre terminología.

Para conocer más sobre el proceso de estandarización del 5G, vea los requerimientos. Algunas de las especificaciones base también incluyen la referencia 23.501 y la 23.502.

Grupo asesor del área de seguridad – Posibilidades de computación cuántica

Kenny Paterson, copresidente del Cryptoforum del IRTF y reconocido experto en cifrado de la Universidad Royal Holloway de Londres, cuestionó el revuelo por la computación cuántica e incluso propuso la provocadora idea de que el énfasis (y el dinero) puesto en las tecnologías cuánticas podría representar una distracción del hecho de que la criptografía en la red no se encuentra en buenas condiciones hoy en día. Paterson hizo referencia a las mediciones a gran escala que expusieron "muchos parámetros Diffie-Hellman que tienen una procedencia desconocida" y "defectos importantes" descubiertos en TLS causados por malas implementaciones.

Cripto-apocalipsis: ¿ahora o nunca?

Por otro lado, era difícil predecir un posible "criptocalipsis" mediante computación cuántica. De hecho, las predicciones de la última década sobre que la computación cuántica era inminente no se cumplieron.

El anuncio de IBM sobre la máquina de 17 Quibits en 2017 más bien ilustró las limitaciones persistentes. Una máquina de 17 Qubits era un notable éxito de ingeniería, dada la inestabilidad de los Qubits con respecto al ruido, el calor, y otros factores inconvenientes. Aun así, los 17 Qubits no permitirían una amenaza a la criptografía de última generación. Según Paterson, los únicos que eran capaces de decir cuán avanzada realmente estaba la tecnología eran aquellos que trabajaban en ese campo, aunque ellos también tenían un interés propio en hacer que el campo se mantuviera con vida.

Paterson le dijo a quien escribe que estimaba que habrá una computadora cuántica en algún momento de su vida que sería capaz de factorear números RSA de 1024 bits al 10 por ciento. Por otro lado, él es miembro de uno de los equipos que está completando una propuesta para el Proyecto Post-Quantum Crypto de NIST (la fecha de entrega es el 30 de noviembre de 2017). El proyecto apunta a identificar un nuevo algoritmo criptográfico cuántico-resistente. NIST pidió algoritmos de clave pública, esquemas de firma digital y mecanismos de intercambio de claves. Es decir, todas las técnicas de la Infraestructura de Clave Pública (PKI).

Paterson dijo que esperaba propuestas de los varios campos: curvas elípticas basadas en isogenia, curvas basadas en Lattices, curvas basadas en códigos y curvas basadas en ecuaciones de múltiples variantes. "Creo que veremos a las cuatro cajas llenas y luego se pone interesante decidir entre estas cosas, porque son extremadamente diferentes en lo que respecta a su desempeño, madurez, y niveles de confianza", dijo Paterson a quien escribe.

La tecnología a prueba de la computación cuántica, según Paterson, eran las firmas basadas en hash, ya que tenían propiedades muy buenas y bien claras, aunque mucho menos de avanzada (o "de vanguardia", como dijo Paterson).

Para las preguntas relacionadas con la confianza del NIST tras el manipulado ECRNG Dual, Paterson se refirió a la crítica completa de la agencia NIST post-Snowden y a los posteriores cambios organizacionales. NIST, por ejemplo, había decidido contratar a expertos en criptografía para sí misma, con el objetivo de tener más independencia con relación a otras agencias —específicamente la NSA—, dijo. Además, esperaba que la comunidad criptográfica vigilara "como un halcón" la selección criptográfica resistente a los procesos cuánticos.

Enfocarse en la criptografía post-cuántica: ¿una distracción?

Paterson convino en que existía una pequeña probabilidad de que las computadoras cuánticas dejarían obsoleta a toda la criptografía de las claves públicas, pero de todas formas dijo que sería válido reconsiderar todo el dinero, tiempo y esfuerzo dedicado a esto.

Durante la reunión en Praga del IETF, Stephen Checkoway, parte de un grupo más grande de expertos en criptografía que incluye a Matthew Green y Eric Rescorla, presentó sus hallazgos sobre la vulnerabilidad arraigada profundamente en los dispositivos Juniper NetOS. Como seguimiento al anuncio de Juniper sobre que los dispositivos fueron accedidos y un parámetro usado para la computación de Random Numbers para Ipsec había sido cambiado, los investigadores comenzaron un gran proyecto de ingeniería inversa para volver firmware por firmware hasta que encontraron un conjunto de cambios en el software de NetOS, incorporados en 2009. Los investigadores encontraron que, contrario a la afirmación de Juniper, el X9.31 (un segundo PRNG) nunca se usó debido a la reutilización del búfer de salida y la variable del índice global. En caso contrario, la manipulación del parámetro Q no habría tenido importancia. La combinación de vulnerabilidades, todas incorporadas, deliberadamente o no, en la misma versión firmware de 2009, hizo que todo el tráfico a través de las VPN que emanaba de los dispositivos NetOS fuera vulnerable.

Paterson, por lo tanto, concluyó que "es útil dirigir una gran cantidad de fuentes de investigación académica y científica hacia algo (computación cuántica) que puede o no ser importante algún día, dependiendo de lo que suceda con la computación cuántica a gran escala. Pero esto nos mantiene ocupados aquí, mientras que toda la acción verdadera en lo que concierne a la seguridad de Internet está en otro lado".

El DNS

Las diferentes variantes para el transporte del DNS se debatieron durante la reunión de Praga en varios WG (vea los "aspectos destacados", más arriba), lo que causó que el director de área de OPS, Warren Kumari, bromeara acerca de la necesidad de contar con un nuevo WG llamado "DNS sobre nuevo Transporte" (DONT, en inglés).

Si bien estas varias propuestas de transporte y la implementación del DNS sobre TLS parecen ir en dirección a la privacidad, también existen varios drafts actuales sobre la lista de debate del WG de las DNSOP que parecen moverse en dirección contraria (vea también los “aspectos destacados”). El WG de las DNSOP investigó una vez más una lista bastante extensa de propuestas y, actualmente, está considerando mantener una pequeña reunión interina sobre temas aislados.

Un draft relacionado con el tema del transporte es el de señalización de la sesión. Se supone que habilita la señalización de la sesión en lugar de por paquete para reducir la sobrecarga que resulta de los mecanismos de señalización por paquete (EDNS0). Aunque todavía sigue en pie el debate sobre el formato del código de operación, los autores de ISC, Apple, Sinodun y Salesforce proponen un nuevo formato para el TLV (tipo-longitud-valor, en lugar de Códigos RR). El nuevo formato requerirá actualizaciones para todo tipo de herramientas (registro, formatos de almacenamiento, y cualquier herramienta que quiera procesar un mensaje del DNS). La RFC brindará una primera lista de mensajes TLV.

Sara Dickinson de Sinodun dijo, durante la presentación, que en cierta forma la señalización de la sesión cambiará el formato del mensaje estándar del DNS (RFC 1035). Incluso surgieron preguntas sobre si este tipo de desarrollo dispararía cuestiones acerca de un diseño mejor definido para un DNS2.

Ondřej Surý, CZNIC, expresó que ocurrió un problema con la implementación del nuevo formato, pero también remarcó que muchas mejoras del DNS, como la del relleno, serían dejadas a un lado. Christian Huitema preguntó cómo encajaría la solicitud de procesar los mensajes “en orden” con Quic (o incluso UDP), que procesan los mensajes a medida que los reciben. El draft sigue siendo materia de debate y podría convertirse en el tema de una pequeña reunión interina.

Los problemas en la agenda de las DNSOP también incluyen a las actualizaciones de los estados de varios drafts.

“La RFC 5011 de Consideraciones sobre Seguridad” deja en claro los tiempos de espera para el uso de nuevas claves de las DNSSEC cuando estas son implementadas. Describe la “matemática detrás del tiempo mínimo que debe esperar un publicador de zona DNS antes de firmar con DNSKEY añadidas recientemente, y también el tiempo mínimo que debe esperar un publicador de zona DNS luego de publicar una DNSKEY revocada antes de poder asumir que todos los resolutores activos de la RFC5011 deberían haber visto la clave revocada y haberla eliminado de la lista de anclas confiables”. La versión actual del draft aclara que existe un tiempo de espera de incorporación (sobre cuánto tiempo debe publicarse una nueva clave antes de que se pueda usar solo esa) y un tiempo de espera de eliminación. La actual implementación de la KSK de la zona raíz está en marcha. En línea con las consideraciones sobre seguridad, tiene 30 días de espera para la incorporación, la antigua validación de 21 días del RRSIG, y dos días de la antigua DNSKEY del TLS. Usando los cálculos de la 5011, serían 56 días. Este tiempo es mucho menor al planificado por ICANN para la implementación de la KSK. Lo mismo sucede con el tiempo de revocación: según los nuevos tiempos de la 5011, el tiempo de mantenimiento sería de 26 días (se eliminan los 30 días

de tiempo de espera para la incorporación). ICANN anunció que el tiempo de espera para eso es de 70 días.
Las preguntas que surgieron incluyeron la duda de si se debía utilizar un tiempo de intervalo o tiempo real para el tiempo de espera de incorporación. Wes Hardacker opinó que el documento ya estaba listo para la última llamada.

El formato de captura de paquetes del DNS (C-DNS) busca facilitar el almacenamiento y las transmisiones de grandes capturas de paquetes mediante el emparejamiento de preguntas y respuestas, y la reducción al mínimo del tamaño de los archivos de capturas de paquetes. Al mismo tiempo, se deben conservar los contenidos completos de los mensajes DNS junto con los metadatos más útiles sobre el transporte. El formato de captura tiene como objetivo ayudar a las aplicaciones de monitoreo del tráfico. Una de las preguntas abiertas fue qué hacer con los paquetes malformados. Los autores también le pidieron al WG que abogaran por los casos de uso adicionales (y los datos que ellos quieren que sean capturados). La situación de los derechos de propiedad intelectual (los DPI corresponden a ICANN) aún no está clara.

El draft "Terminología del DNS " se debatió durante un corto tiempo y Paul Hoffman pidió una revisión extra para darle la forma definitiva. Este documento será el sucesor de la RFC 7719, dejándola así sin vigencia. Puede que se necesite un tercer documento. Los presidentes de DNSOP consideraron que el draft sobre terminología era uno de los posibles temas para una pequeña reunión interina.

Se debatió una actualización prevista para la RFC 2845 como respuesta a la reciente vulnerabilidad TSIG en BIND y Knot. Los proveedores de DNS que se reunieron en Praga decidieron que la sección 4.5 fue la fuente del error de implementación que resultó en la vulnerabilidad TSIG.

Las negociaciones de algoritmos en las DNSSEC deberán permitir que los clientes del DNS especifiquen, en orden de preferencia, qué algoritmos quieren emplear. Los servidores que respondan deberán utilizar el algoritmo que puedan soportar que sea preferido por el cliente. Al mismo tiempo, deberán permitir la elección del soporte de los algoritmos y la flexibilidad de estos.

Se puede ver aquí una lista actualizada sobre los muchos documentos tenidos en cuenta en el WG del DNS.

DPRIVE

En DPRIVE, además del DNS sobre Quic (vea los "aspectos destacados"), se dieron notables presentaciones sobre relleno ("padding") y Demux.

En relación con el draft sobre relleno, presentado por Alex Mayrhofer, nic.at, existió un breve debate sobre la nueva "estrategia recomendada". Tras las observaciones, se debatió brevemente la preferencia (o no) del relleno completamente aleatorizado que evitaría el análisis del conteo de bloqueos, pero la idea fue rechazada, por ahora... Daniel Kahn Gillmor (ACLU), quien analizó el

impacto del relleno, revisó los verdaderos rastros de paquetes de los resolutores de Surfnet, aplicó una simulación de relleno al paquete y se presentó con la recomendación de que uno debería rellenar las consultas en un bloque de 128 bits de tamaño, y las respuestas en 468 bits. El relleno de 128⁄468 implica que el 93 por ciento de los paquetes tienen exactamente el mismo tamaño. El "costo" también fue calculado por DKG, basándose en un atacante que está interesado en una consulta-respuesta — ¿cuánto de los otros paquetes se encontraría en un cubo del mismo tamaño? El relleno aleatorio, que algunos recomiendan, sería mucho más difícil y podría convertirse fácilmente en un relleno pseudo-aleatorio y filtrar datos. En el futuro, las políticas de relleno podrían cambiar, pero el draft sería un buen punto de partida necesario para evitar que los implementadores se muevan en distintas direcciones (que pueden ser propensas a fallas).

El WG de DPRIVE también tomó en cuenta una propuesta controvertida de DKG (ACLU) para el DNS sobre TLS sobre "inclinarse al puerto 443" para hacerlo indiscernible del tráfico https. Un simple "servidor demultiplexor" debería distinguir entre los paquetes que llegan de DNS y HTTP, basándose en los primeros bytes enviados por el cliente en un flujo determinado; una vez establecida la elección, el resto del flujo se dedica a una u otra interpretación. DKG cuenta con una implementación en un servidor Debian, pero reconoció que fue "la peor idea del día" (y que el DNS sobre https sería la mejor solución).

Los drafts de TLS y DTLS están en la etapa de revisión del IESG. El siguiente paso —la privacidad en el camino del resolutor al autoritativo— todavía queda por abordar.

Homenet: ¿el documento de simple nombrado está "casi listo"?

Luego de estar estancado por algún tiempo debido a la delegación de un "TLD especial" el WG de homenet ahora espera avanzar, pero todavía tiene bastantes problemas por resolver. Las relaciones del trabajo en el DNSSD ahora se describen en un documento guía que intenta brindar una visión general del statu quo del descubrimiento de servicios en las zonas locales y de redes domésticas. El WG de homenet cuenta con una nueva copresidente, Barbara Stark, de AT&T, quien remplazará a Mark Townsly (Cisco), mientras que Ray Bellis (Nominet) permanecerá en su cargo. Curiosamente, Stark hizo un comentario que cuestionó la afirmación "el DNS es uniforme". Expresó que el DNS no es uniforme, o al menos que este concepto no es adecuado (para los espacios de nombres paralelos del DNS global y homenet).

La nueva elección para el dominio homenet, homenet.arpa en lugar de .homenet, está camino a ser definitivo luego de las rondas adicionales realizadas con esfuerzos puestos en el comportamiento de homenet.arpa y las DNSSEC. Para abordar el dilema de que los resolutores que validan las DNSSEC podían desechar consultas para lo que consideran como delegaciones inseguras, la versión 11 del "Uso del Dominio Especial 'home.arpa'" prohíbe el reenvío recursivo de consultas example.homenet.arpa "a servidores fuera de los límites lógicos de homenet con la excepción de búsquedas DS para 'home.arpa.'"

Habiendo resulto finalmente el debate sobre el TLD especial, Ted Lemon intentó dar un paso

adelante con respecto al nombrado y al descubrimiento de servicios durante la reunión en Praga. El draft que propuso al WG para que fuera aceptado como un documento del WG, "Nombrado simple de homenet y la arquitectura del descubrimiento de servicios", combina la búsqueda de dominios en Internet, publica los servicios alcanzables desde cualquier lugar en la red doméstica y descubre los servicios en la red doméstica.

Lemon declaró que los siguientes no son objetivos por ahora:

- publicar una zona DNS para homenet en el DNS
- poner a disposición el descubrimiento de servicios fuera de homenet
- permitir que los servicios fuera de homenet publiquen servicios en homenet
- asegurar que homenet utilice las DNSSEC

Explicó que el desafío pendiente es el *multihoming*, pero que los demás problemas ya estaban siendo abordados en una serie de documentos, que no se debatieron en detalle durante la sesión de Praga:

+ draft-sctl-service-registration-00 Según este draft, el Protocolo de Registro de Servicio del DNS-SD deberá brindar "una manera de llevar a cabo el Descubrimiento de Servicios Basados en DNS utilizando paquetes de unicast". Se elaboró "en gran parte a partir de la Actualización del DNS [RFC2136] [RFC3007], con algunos agregados".

+ draft-sctl-discovery-broker-00 "El Bróker de Descubrimientos es un intermediario entre los dispositivos del cliente y los Proxies de Descubrimiento. Es una suerte de conmutación de barras cruzadas multiplexadora. Protege al cliente de tener que conectarse a múltiples Proxies de Descubrimiento, y a su vez protege a estos últimos de tener que aceptar conexiones de miles de clientes".

+ draft-sctl-dnssd-mdns-relay-00 Según los autores, esto extiende al actual proxy de descubrimiento para el descubrimiento de servicios MDNS describiendo una transmisión de descubrimiento "que permite a los proxies de descubrimiento brindar servicios en enlaces a los que los hosts en los que están funcionando están directamente conectados". Las dos partes del protocolo son: "Las conexiones entre los Proxies de Descubrimiento y las Transmisiones de Descubrimiento, y las comunicaciones entre las Transmisiones de Descubrimiento y los agentes mDNS".

Hubo cierto apoyo por parte del WG, aunque el tema se debatió considerablemente. Con respecto al *multihoming*, Andrew Sullivan preguntó por qué un host debería contar con una teoría con respecto a qué ISP dirigirse en un escenario de *multihoming*. Su inquietud, explicó, residía en que según la manera en la que funciona el documento de nombrado en este momento, el host (al menos, y quizás también la aplicación) necesita contar con una teoría sobre cuál ISP se utilizará para una conexión. Esto no sucedería, y las ideas sobre este trabajo que presentó el grupo de MIF que podían ser de ayuda eran más "una esperanza que un plan". Aún quedaba mucho trabajo por hacer en el documento de nombrado.

La nueva copresidenta, Barbara Stark y David Schinazi propusieron la idea de que Happy Eyeballs podría resolver el problema.

Juliusz Chroboczek y algunos otros hablaron de “muchas piezas sueltas” en los documentos. La hoja de ruta preparada por Stuart Cheshire, presentada en DNSSD, instó a un cambio significativo en el campo de la red doméstica/local al proponer alejarse de la transmisión multicast hacia una completamente unicast.

Otra presentación de Lemon abordó preguntas sobre cifrado en la red doméstica. Aunque no existe hasta el día de hoy un draft escrito sobre esto, Lemon propuso que cada uno de los nodos de homenet debería generar un par de claves privada-pública y distribuir las partes de la clave pública a los nodos de homenet. Esto permitiría el uso de DTLS, en lugar de solo contar con el enfoque de secreto compartido ahora disponible en el Protocolo de Control de Homenet (HNCP).

Si bien recalcó que el solo enfoque de la PKI no traía seguridad, sí permitiría la identificación de los nodos con los que uno se comunique. Hubo cierto apoyo para abordar el problema. Algunos participantes recomendaron considerar la seguridad/cifrado del sistema bancario para incorporarlos en las especificaciones base. Sin embargo, Lemon argumentó que el draft sobre claves podría terminarse mucho más rápidamente, así que tendría sentido hacer una división.

Lemon habló de un intento para implementar homenet para un escenario homenet de doble enlace (dual-homed), lo cual reveló problemas importantes. De las tres implementaciones disponibles en el HNCP (protocolo de control de homenet) (hnetd, pysyma, y shncpd), Lemon escogió a hnetd para OpenWRT y a shncpd para Ubuntu. Tras la configuración, el enrutador OpenWRT perdió su corriente de direcciones Ipv4 debido a que el DHCP ya no la habilitaba, y “el prefijo de la RFC1918 sobre el Ipv4 que había asignado fue desconfigurado en todas las interfaces sin motivos evidentes”. Si bien varios participantes señalaron que OpenWRT les estaba funcionando de manera correcta, otros recomendaron analizar estos problemas en profundidad.

Homenet y DNSSD: ¿aún son diferentes?

Homenet y DNSSN parecen acercarse en temas de trabajo, al menos compartiendo postulados: El DNSSD intenta hacer funcionar el descubrimiento de servicios de manera correcta a través de más que solo la red de vínculo local, mientras que Homenet toma como postulado de base que “homenet” podría ser (no debe, sino que podría) ser multi-homed, en cuyo caso, algunas cosas no se encuentran *siempre* en el enlace local.

DNSSD: lejos de multicast y con mejor privacidad

En la reunión de Praga, Stuart Cheshire recomendó alejarse de la transmisión multicast para el descubrimiento de servicio DNSSD y manejo de brokers. Aún debería apoyarse la transmisión

multicast para no dejar atrás a los dispositivos que lo han estado usando por 15 años. No obstante, este concepto sobrecargó a las grandes redes de compañías con cientos de clientes de Wifi y también redes domésticas (homenets) con más de un enlace. Por lo tanto, el grupo debería despegarse de multicast y adoptar únicamente la transmisión unicast.

En una hoja de ruta, Cheshire describe el escenario para los servicios DNSSD en evolución, con descubrimiento de servicios y registro de servicios, y especialmente un nuevo concepto para un "bróker de descubrimiento" central.
El bróker que presentaron Ted Lemon (Nominum) y Cheshire deberá permitir el empaquetamiento de múltiples dominios en uno solo y dirigir las consultas de diferentes clientes hacia este, en lugar de distintos descubrimientos de servicio. El bróker funcionaría como un servidor de meta-descubrimiento, aceptando las consultas de servidores externos y realizando consultas a los varios servidores de descubrimiento para ellos. Para los servidores de descubrimiento, el servidor de meta-descubrimiento/empaquetado/bróker se ve igual que un cliente. Esto hace más jerárquica la red doméstica/local. Cheshire llegó a decir que no deberían elaborar dos documentos abocados a extender las publicidades de multicast a través de enlaces.

Sin embargo, se debería asegurar la compatibilidad hacia atrás en las funciones de descubrimiento. Cheshire y Lemon están considerando dividir las funciones para descubrimiento en un bróker de descubrimiento y una transmisión de descubrimiento, siendo esta última moldeada en base al concepto de red de compañías de servidores DHCP núcleo.

Para el registro en el espacio de nombres, los dispositivos antiguos del mDNS serán capaces de utilizar un descubrimiento de servicios híbrido de DNSSD (draft-ietf-dnssd-hybrid-06). Según Cheshire, el documento depende de DNSPush (para la notificación de cambio asíncrona en lugar del sondeo) que a su vez depende de la señalización de la sesión del DNS, que se encuentra en un caluroso debate en las DNSOP (vea más abajo).

Para el registro activo de dispositivos, se incorpora un nuevo protocolo de registro de servicios en otro documento nuevo (sctl-services-discovery) con autoría de Cheshire y Lemon. Está basado en la actualización del DNS (RFC 2136). Una opción de EDNSO se utiliza para especificar qué información adicional debería transportarse (servidor dormido y un patrón de bit Magic Pattern Wake-on-LAN que se puede emplear para despertarlo) para permitir la eficiencia energética o el ahorro energético, respectivamente.

Finalmente, algunos participantes del WG CoRE presentaron los trabajos realizados en el descubrimiento de recursos CoRE y promovieron un documento sobre un mapeo de descubrimiento DNSSD y mecanismos de descubrimiento CoRE que ya está en vigencia. El descubrimiento de recursos CoRE y el toscamente veteado descubrimiento de servicios DNSSD eran complementarios "en el caso de grandes redes, en las que el último puede facilitar la escalabilidad". Según los autores, este documento definirá "un mapeo entre los atributos del Formato de Enlace CoRE y los campos del Descubrimiento de Servicios Basados en DNS [RFC6763] que permita el descubrimiento de servicios CoAP por cualquiera de los dos métodos".

Mejoras en la privacidad

Antes de la presentación de la siguiente ronda de drafts para el "nuevo" camino de DNSSD, Christian Huitema presentó los dos drafts relacionados con la privacidad para DNSSD. Para mejorar la privacidad, los nodos publican nombres de instancia (hashes) por cada emparejamiento que llevan a cabo. Utilizando el secreto compartido, dan comienzo a las sesiones TLS. Este concepto se prefirió a un sistema PKI, según Huitema, al revisar la lista de problemas, debido a que la clave pública era un identificador único y sería revelada durante el *handshake* del TSL. La PKI brindaba una autenticación del cliente implícita. El concepto del secreto compartido, por otro lado, permitía un intercambio anónimo.

Otro de los temas que se debatieron fue la sincronización de los espacios de tiempo, en la que los nodos publicaban nombres de instancia cada cinco minutos. La sincronización hasta intervalos de aproximadamente 4 minutos fue necesaria para evitar que los nonces/hashes se volvieran obsoletos. Surgió una pregunta sobre cuánto tiempo se podría estirar el intervalo para facilitar el uso. Huitema defendió la opción del intervalo corto, y argumentó que el nonce basado en tiempo controló la carga computacional y mitigó los ataques DOS. Agregó que estirar la validez daría paso a los dispositivos de seguimiento de camino a sus redes. Para atenuar los posibles problemas en los límites de los intervalos, durante el primer minuto de un nuevo intervalo, se debió verificar el viejo hash, y durante el último minuto de un intervalo, se debió verificar el nuevo hash.

Más posibilidades de *fingerprinting* resultan de la publicación de tantas instancias como de emparejamientos. Al contar el número (y unirlo a las instancias publicadas), el *fingerprinting* podría ser posible. Una reacción posible podría ser el rellenado con instancias falsas. Un draft adicional propone usar códigos QR como alternativa para el descubrimiento y la verificación. La pregunta para el WG fue si los códigos QR deberían formar parte del draft principal o permanecer en un draft especializado. El WG todavía debe tomar la decisión sobre cómo dividirlo, lo que probablemente se transforme en tres documentos: análisis del problema, especificación del emparejamiento y especificación de los códigos QR.

La próxima reunión del IETF (IETF100) tendrá lugar del 11 al 17 de noviembre de 2017 en Singapur.