Informe de CENTR

IETF 103

Bangkok, 3 - 10 de noviembre de 2018

Traducción - LACTLD

LACTLD agradece a Hugo Salgado (NIC Chile) por la revisión de la edición en español

Para acceder a la versión en inglés de este informe, visitar https://centr.org/library

LACTLD
Latin American and Caribbean ccTLDs Organization

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Contenidos

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Aspectos destacados

Las revisiones sobre derechos humanos no son bienvenidas en algunos espacios del IETF

El Grupo de Investigaciones sobre las Consideraciones de Derechos Humanos en los Protocolos (RG de HRPC, por sus siglas en inglés) comenzó a llevar a cabo revisiones más frecuentes en los protocolos emergentes desde el punto de vista de los derechos humanos (se analizan problemas de privacidad, pero también la accesibilidad y los efectos de la internacionalización o la concentración del mercado). Durante la semana del IETF en Bangkok, dos revisiones en particular resultaron en debates intensos que dejaron perplejas a las ONG que llevaron a cabo las revisiones. La exmiembro del Parlamento Europeo, Amalia Andersdottir, que ahora trabaja en Article19, habló sobre «mensajes confusos» que eran difíciles de explicar. Algunos grupos de trabajo (WG), como Suit o IPWave, recibieron favorablemente las revisiones, pero la presidenta del IETF, Alissa Cooper, y el director saliente de Área de Seguridad y miembro del IESG, Eric Rescorla, desacreditaron firmemente el informe realizado a QUIC.

El informe del RG de HRPC realizado a QUIC pareció ser inútil a los ojos de la presidenta del IETF

La revisión de derechos humanos del nuevo protocolo de QUIC recibió la peor crítica durante la sesión del RG de HRPC en la reunión IETF103.

Según la directora del Área de Transporte, Mirja Kühlewind (ETH Zurich), la revisión no agregó temas de discusión para el grupo de trabajo de QUIC. Dicha revisión estaba llena de errores técnicos y se alejaba demasiado del trabajo de estandarización, según el director del Área de Seguridad, Eric Rescorla. La presidenta del IETF, Alissa Cooper, agregó que la revisión, en esencia, carecía de intervenciones directas hechas por expertos en el tema en el WG, y resaltó, en cambio, el «gran trabajo» del IETF en cuanto a la mejora de la privacidad en los últimos años.

Cooper también señaló que los debates sobre «Revisiones de Privacidad» para los *drafts* de los talleres que se habían propuesto en su momento no habían llegado a nada. Las Revisiones de Privacidad, una idea basada en el trabajo previo a Snowden sobre las «Consideraciones de Privacidad en Protocolos de Internet» (RFC 6973), estaban destinadas a ser llevadas a cabo por los miembros del Área de Seguridad del IETF. Sin embargo, debido a que el Área de Seguridad ha estado mucho menos activa últimamente, en parte por el volumen de trabajo de sus presidentes (Eric Rescorla es autor activo de *drafts* y se convirtió hace poco en el director de tecnología de Mozilla), hace mucho tiempo que no se llevan a cabo revisiones de privacidad formales.

Niels Ten Oever, cofundador del Grupo de Investigación (GI) de HRPC y coautor de la revisión de QUIC (entre otras) recibió bien las opiniones, y anunció que esto ayudaría a informar el trabajo en un documento de directrices sobre cómo deben llevarse a cabo las revisiones de derechos humanos en el futuro. El documento enumera cinco métodos (también utilizados en la revisión de QUIC):

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

- Analizar los *drafts* en base a las directrices en el modelo de consideraciones sobre derechos humanos
- Analizar los *drafts* en base a su posible repercusión
- Realizar entrevistas con expertos
- Realizar entrevistas con las comunidades afectadas
- Rastrear las repercusiones

Ten Oever indicó que las entrevistas fueron un fiel reflejo de los debates de los grupos de trabajo y anunció que se podría reconsiderar este punto. Hablar con expertos, por otro lado, permitiría que el RG de HPRC se ocupe de los detalles técnicos del *draft* tanto como le sea posible.

La pregunta básica para el GI de HRPC ahora es cómo seguir adelante. Dados los comentarios hostiles, podría ser más difícil encontrar personas que lleven a cabo las revisiones. A su vez, los ingenieros que trabajan en los *drafts* de estándares, por lo general, están muy ocupados para terminar los *drafts*. ¿Puede arreglárselas el IETF sin la revisión externa sobre privacidad y otras repercusiones de la tecnología que causan los estándares? Cooper parece sugerir que sí. Sin embargo, las revelaciones de Snowden y la reacción del IETF ante esto en su trabajo de privacidad intensificado parecen indicar lo contrario.

El debate acalorado sobre la revisión de derechos humanos en la extensión de verificación del RDAP en el WG de RegEXT

Los documentos sobre QUIC debatidos intensamente no fueron los únicos *drafts* que se enfrentaron a una revisión de derechos humanos. Esta vez, el WG de Extensiones de Registro recibió una evaluación con respecto a la extensión de verificación del RDAP. El informe de HPRC enumeró los puntos que debe tener en cuenta el WG. Los primeros tres fueron los siguientes:

Con respecto a la privacidad: Los VSP (proveedores de servicio de verificación que actúan como terceros) están obligados a («DEBEN») recopilar y almacenar los datos personalmente identificables (el nombre de dominio, el contacto del solicitante).

Con respecto al control de contenido o la censura: Los VSP verificarán «si el nombre de dominio no está prohibido o si el solicitante representa a una organización individual válida, o a un negocio en la localidad».

DPI: ya que el IETF favorece los estándares abiertos, partes de la especificación están cubiertas por una patente solicitada por VeriSign. Según la revisión, «esto incluye una descripción del periodo de gracia en el que los requisitos establecidos sobre los códigos de verificación se pueden enviar antes de que el objeto deje de cumplir con las normas», y «una clara representación del flujo de la solicitud que se detalla en la Figura 1 de la [PATENTE]».

En resumidas cuentas, quienes llevan a cabo las revisiones decidieron que el *draft* del estándar tenía problemas y recomendaron que el WG sea, por lo menos, transparente acerca de los riesgos en una sección de consideraciones sobre derechos humanos. Dicha sección debería agregarse, junto con la seguridad estándar y la privacidad opcional, al final del texto de especificación. También recalcaron que el WG podría considerar no convertirlo en un estándar

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

completo desde el comienzo, ya que hasta ahora solo una compañía (VeriSign) lo está aplicando. En ese sentido, la extensión, en esencia, no cumple con el proceso del IETF, debido a que toma varias aplicaciones independientes llegar a la calificación de «estándar».

Tras una discusión controvertida previa en la lista de mails, el presidente del WG, Jim Galvin, reservó algo de su tiempo en la reunión en Bangkok. Ambas partes pudieron avanzar hacia un posible consenso en cuanto a los problemas. El autor y editor de documentos James Gould admitió un problema concerniente a la obligación de los VSP acerca de la retención de datos personalmente identificables, y efectuó un cambio en la declaración de este asunto acorde a la legislación local. Los VSP necesitan almacenar su decisión de validación para el solicitante del dominio. El almacenamiento de datos adicionales (nombre, dirección del solicitante) está sujeto a la legislación de privacidad local.

Aparte de eso, Gould dijo que no se sentía lo suficientemente competente para agregar una «sección de consideraciones sobre derechos humanos» que, según lo propuesto, resaltaría los posibles riesgos en cuanto a privacidad, discriminación y accesibilidad. Su colega de VeriSign, Scott Hollenbeck, cuestionó la idea de consideraciones sobre derechos humanos «estándar» en los *drafts* de las RFC. Dijo que no había política de consenso en el IETF sobre este punto y que el WG de RegEXT no debería ser la experiencia piloto.

El presidente del RegEXT, Galvin, recalcó varias veces que las consideraciones solo podrían tomarse como contribuciones individuales, de la misma forma que se toma cualquier otra contribución técnica en cuestiones tecnológicas. Galvin hasta llegó a decir que el WG debería concentrarse solamente en la tecnología, ya que los asuntos de políticas estaban fuera del proceso. Ten Oever cuestionó duramente esa afirmación y dijo que sería ingenuo considerar a la tecnología y la estandarización neutrales en lugar de políticas.

Búsqueda inversa: ¿el próximo candidato para la revisión de derechos humanos/privacidad?

Quizás una mejor visión de cómo las normas son políticas en parte, fue entregada por el propio WG en su discusión sobre la extensión de búsqueda inversa RDAP. Loffredo (.it Registry) presentó la extensión, que permitiría una búsqueda inversa en la base de datos RDAP a partir de varios puntos de datos, como candidato para un nuevo hito. La extensión de búsqueda inversa está dedicada principalmente a los registradores, permitiéndoles buscar sus propios dominios y debería proporcionarse bajo un estricto control basado en los niveles de acceso de los usuarios. Tras completar la mayoría de sus hitos (ver a continuación), el WG ha reformulado su carta constitutiva y está abordando nuevos documentos de extensiones para la próxima iteración.

Al presentar la propuesta, el propio Loffredo mencionó las políticas de ICANN, en específico dos documentos producidos por ICANN: el RDS de la próxima generación (2014) y las especificaciones para el Acuerdo de Registro (2017). El presidente Galvin señaló que hay muchas discusiones actuales sobre el despliegue de RDAP, y que el trabajo del WG no puede estar motivado sólo por las políticas de ICANN. Wilhelm (Verisign), miembro del WG, advirtió que uno de los documentos citados (el RDS de la próxima generación) había sido clausurado y que el borrador estuvo en las implementaciones muy iniciales de RDAP, dado que la comunidad de ICANN estaba aún trabajando en políticas de registro post GDPR. Así pues, este tipo de cosas

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

ocasionan una carga en la implementación para las partes contratantes. Aunque Alvarez (ICANN) solicitó contar con capacidades de búsqueda inversa durante la sesión, una capacidad de búsqueda inversa descontrolada podría potencialmente tener un impacto en algunos aspectos de privacidad. Finalmente, Loffredo respondió que el *draft* no estaba solo influenciado por las políticas de ICANN y que los autores estaban pensando en tomar un enfoque controlado en la búsqueda inversa.

El principal mensaje con respecto a la relación de los estándares y la política es que, de vez en cuando, son tanto las políticas de los ccTLDs y de los gTLDs las que se mencionan en cuanto a la legitimación del trabajo de los estándares. El RegEXT es quizás uno de los grupos que mejor demuestra cómo el trabajo de los estándares técnicos traza una fina línea entre los estándares y las políticas.

La decisión de incluir la búsqueda inversa y otras propuestas que actualmente solicitan aplicación en la nueva carta constitutiva (ver a continuación) se tomará en la lista de mails o durante la próxima reunión del RegEXT.

No queda claro si el WG de RegEXT volverá a las recomendaciones del RG de HRPC. Durante el debate del WG, Ulrich Wisser, de ISS, argumentó que hacer transparentes los posibles problemas de privacidad en una sección corta era «apenas suficiente». Es casi seguro que los miembros del HRPC presentes en el WG volverán con más revisiones (probablemente sobre la búsqueda inversa). El WG de RegEXT, un grupo relativamente pequeño, seguramente solicitará más revisiones de sus documentos, que afectan a millones de solicitantes en el mundo.

¿Un consenso general? La sesión plenaria del IETF recibió quejas sobre los tratos agresivos en los debates de los WG

Bastó con un breve comentario de uno de los responsables de instruir a los nuevos participantes del IETF para abrir las compuertas de un debate extendido similar al MeToo sobre el comportamiento a menudo agresivo en los grupos de trabajo del IETF. Wes Hardaker dijo que le habían contado historias impactantes, mientras leía un comunicado cuidadosamente redactado en la sesión plenaria. Si bien dijo haber estado fascinado por la gran pasión que notaba en las reuniones, luego comprendió que dicha pasión existía a costas de otros, y recordó los nervios que sintió la primera vez que habló en un WG del IETF. Hardaker instó a los participantes del IETF a expresar más cuidadosamente sus contribuciones, incluso al momento de hablar con los ingenieros más experimentados del IETF, y sin importar cuán fuertes piensen que pueden ser aquellos que participan en los debates.

Adam Roach, director de área en WebRTC y observador de los debates de RegEXT, intervino y mencionó que ahora había más sensibilidad que antes, y fue en ese momento que los comentarios comenzaron a aumentar y algunos advirtieron que el problema no se había abordado y que, de hecho, había empeorado.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

DNS sin resolutor y otros próximos pasos del DoH

Dados los acalorados debates que suscitaron el DNS sobre HTTPs y la prueba actual de Mozilla, no se habló mucho de estos temas en el IETF en Bangkok. Aun así, parece que el DNS se ha convertido en un área controvertida.

Patrick McManus le dijo a quien escribe que sintió que la operación de la prueba de Mozilla había sido caracterizada erróneamente y que se debatirían los próximos pasos. Una docena de servidores del DoH (que incluyen Cloudflare, Quad9, Google, PowerDNS) están disponibles al público actualmente según el proyecto paralelo GitHub DOH. El proyecto de Privacidad del DNS lleva un registro y observa que Chrome estaba «trabajando en la exposición del DoH a través de la opción de configuración del usuario con una lista desplegable y una opción definida por el usuario».

El WG de DoH, con la publicación de la RFC 8484 «Consultas DNS sobre HTTPS (DoH)», quedó inactivo, esperando decidir si debería reformular su carta constitutiva. Según uno de los presidentes, el posible trabajo de seguimiento podría llevarlo a cabo DNSOP, DPRIVE o httpbis. En algunas instancias, sin embargo, podría ser necesaria la combinación del conocimiento del DNS y HTTP. Bert Hubert (Power DNS) dijo en la lista de mails que el DoH en su forma actual no es eficaz, ya que los usuarios necesitan «alrededor de 22 paquetes por consulta/respuesta DNS». Hubert observó que TLSv1.3 podría mejorar este punto y que «una red “levemente subóptima” mata por completo el desempeño de navegación en Firefox Nightly usando el DoH» (una pérdida de paquete del 0,5% se traduce a una tasa de fallas del 5% por consulta DoH). Hubert, uno de los críticos del DoH, solicitó considerar un *draft* sobre una versión DoH3.

Paul Hoffman (ICANN) presentó una propuesta sobre cómo se podría organizar la opción de un resolutor DoH para un usuario de DoH durante la sesión del grupo de trabajo de DNSOP. Hoffman expresó que eran las primeras etapas de la propuesta. Al menos un desarrollador del «lado web» le dijo a quien escribe que era más probable avanzar con otros conceptos, como el propuesto en la BoF de DRIU en la reunión IETF102. El DRIU analiza elegir servidores DoH al azar (el concepto del filtro de Bloom).

Simultáneamente, una idea de confiar en que los servidores impulsen respuestas adicionales vía “push” (para algunos registros DNS) podría formar parte de próximas propuestas.

Una reunión paralela sobre el DNS sin resolutor

Otra idea para la posibilidad de extraer respuestas DNS hacia el mundo web es la del DNS sin resolutor, que básicamente considera cómo responder consultas usando no solo el registro DNS que se busca, sino también información adicional del DNS que se almacena en el cliente local (uno pide example.com y obtiene foo.example.com, dependiendo del alcance y de los dominios fuera de la zona a la que se le pidió originalmente). La idea original la propuso Daniel Kahn Gilmore (ACLU), quien la propuso como una forma de evitar el rastreo de las solicitudes DNS.

Si bien no se ha hecho una propuesta formal en el IETF y la lista de mails sobre DNS sin resolutor ha estado muy silenciosa, la reunión paralela terminó con, básicamente, tres posibles soluciones:

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

1. Con firma DNSSEC, cualquier enlace saliente o “resource” de un sitio
2. Enlaces o “resources” locales al CDN
3. Dentro de TLS: cualquier ”resource” cargado de manera automática

Las propuestas abordan de manera implícita preocupaciones sobre los diferentes mecanismos. Estas preocupaciones incluyen la pérdida de control de adónde se dirige el tráfico (ya que un resolutor DNS ya no está en el circuito) y más preocupaciones sobre seguridad. Si no se despliega DNSSEC ni se adapta al esquema, redirigir el tráfico sería un problema.

Algunos piensan que se podrían utilizar diferentes estándares para aceptar los registros. Los dominios que no estén cubiertos por un certificado del sitio web que los emite podrían depender de la validación con DNSSEC.

Para dar lugar a un poco de control, se debatió la idea de que los mismos nombres de host deberían tener la posibilidad de aceptar o rechazar la emisión de sus nombres por parte de otros servicios.

Sin embargo, todavía hay preocupaciones sobre los ataques de repetición (“*replay*”), balanceo de carga y los dominios que se ven parecidos. Un atacante podría, por ejemplo, ser emitido por un servidor, para enviar fakebook.com en lugar de facebook.com. Además, el balanceo de carga podría verse afectado y podrían fomentarse los ataques de *replay*.

También se debatieron las consecuencias para DNSSEC (la necesidad de ser implementado a nivel del navegador y posiblemente desincentivar la implementación a nivel de sistema operativo).

Hasta ahora, los debates han sido infructuosos. En la lista de mails sobre DNS sin resolutor, se propusieron nuevas ideas como «un nuevo encabezado de solicitud HTTP, por ejemplo “Accept-DNS”» (Justin Henck, Jigsaw), pero queda por verse si se presentará un *draft* formal en el IETF. Ben Schwartz, también de Google Jigsaw y copresidente del WG de DoH, dijo que el concepto de no usar resolutor era muy especulativo por el momento como para adoptarlo en los WG de DNSOP o DoH, y que no veía «ninguna forma de hacerlo dentro del modelo de seguridad de la web».

Hiperlocal a la próxima ronda: RFC 7706 bis

Algunos de los objetivos de la RFC 7706 fueron acortar los tiempos de respuesta, agregar resiliencia y también privacidad. Paul Hoffman (ICANN) le presentó al WG una propuesta para elaborar una versión bis para lo que se denominó «zona raíz hiperlocal» en ICANN.

La RFC 7706 de Hoffman y Kumari (Google) se adoptó en 2015. La idea de base es extraer una copia del archivo de zona raíz para evitar enviar las consultas hacia los servidores raíz. En su lugar, las consultas se pueden responder de manera local (desde un servidor *loopback*, para evitar las respuestas ofrecidas por fuera de la red local).

Varios servidores raíz ya ofrecen la opción de que terceros descarguen el archivo raíz completo.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Hay software de código abierto de DNS que ya ha aplicado el concepto hiperlocal. Ondrej Sury (BIND) informó que BIND incluiría (además de cooperar con ICANN) una copia local de la raíz en la próxima versión. Unbound también usa el concepto de la 7706. Knot experimentó y descubrió que podría ser más eficaz que las soluciones actuales, según Petr Spacek (cz.net). Spacek informó que, actualmente, Knot usa una combinación del cacheo agresivo de NSEC 3 y *prefetching*.

Hoffman dijo que en el nuevo *draft* bis se haría foco en debatir si el servidor raíz necesita estar en una máquina local, o si podría operar por fuera, por un tercero para la distribución hiperlocal. Asimismo, en caso de fallas del servidor hiperlocal, deben tenerse en cuenta mecanismos de emergencia. La RFC 7706 bis también analizará el código en ejecución existente. Un ejemplo de código en ejecución es el proyecto de host local de Wes Hardaker, que permite que las personas instalen resolutores locales con la zona raíz para «servirse a sí mismos».

Más pasos para la privacidad: QNAME, de experimental a estándar

Además del concepto hiperlocal, otra tecnología existente que se actualizará con una versión bis de una RFC es la minimización de QNAME (RFC 7816). La mayor parte del software de DNS ahora la ofrece (BIND la anunciará en las próximas semanas, Knot y Unbound la ofrecen en sus versiones actuales como opción). Con la minimización de QNAME, no se enviarán consultas completas a la zona raíz sino solo aquellas para las zonas TLD, eliminando así la posibilidad de que los servidores raíz sigan el rastro de consultas individuales.

Hubo amplio consenso en que lo lógico sería hacer que la minimización de QNAME sea un estándar en lugar de un experimento. Una vez más, Paul Hoffman (ICANN) prepara la versión bis del documento. Hoffman señaló que, dado que el trabajo de DPRIVE (trabajo que asegura la privacidad desde el resolutor al servidor autoritativo) se estaba quedando muy atrás, tenía sentido impulsar la minimización de QNAME.

Aunque desde afuera las diferentes partes móviles de la evolución del DNS parecen competir, al menos en algunos aspectos, los expertos piensan que superponer las distintas partes (DoH, DoT, la minimización de QNAME, y el concepto hiperlocal) aborda diferentes problemas y podrían ser complementarias. El único problema en este sentido podría ser el esfuerzo (y/o costo) de modificar el DNS propio para que use todos los mecanismos, lo cual puede ser un poco abrumador y solo sería una opción para las organizaciones y compañías más grandes.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Grupos de trabajo

Grupo de trabajo DNSOP

El trabajo más importante actualmente en el WG DNSOP —sin contar los debates en segundo plano sobre DoH y DoT— se trata de cómo facilitar el uso de direcciones específicas de aplicaciones y servicios en un registro DNS.

ANAME o registro http mínimo

Debido a que se considera que los Registros de Recurso de ubicación de Servicio (SRV) no son lo suficientemente fáciles de usar desde una perspectiva web, y dado que los registros CNAME existentes no son lo suficientemente flexibles (porque no permiten ubicar direcciones adicionales en el “apex”), el WG está intentando encontrar una solución. Se debatieron dos propuestas en Bangkok. Una es la creación de un nuevo registro de recurso llamado alias DNS de dirección específica (Address specific DNS aliases, ANAME). En apariencia ANAME se parece a CNAME, pero está diseñado para estar en el “apex”.

Ray Bellis (ISC) ahora propone otro registro de recurso que él denomina un tipo de registro de recurso destinado al «HTTP mínimo». Debería «facilitar la redirección desde la porción del nombre de dominio de un URI HTTP(s) al servidor del nombre del host y, desde allí, a registros A o AAAA». A diferencia de ANAME, este registro remplazaría a CNAME por completo.

El debate sobre estas cuestiones todavía no ha terminado y, hasta ahora, ha sido infructuoso.

Blockchain vinculado con DNS - DNS DID

Un tema con visión a futuro en el WG del DNS (también presentado en el Grupo de Investigación de Infraestructura de Internet Descentralizada) se trata de qué podría ofrecerles el DNS a los proveedores de blockchain.

Con respecto a la interoperabilidad, el W3C ya ha comenzado a trabajar y ha brindado un esquema URI que permite direccionamiento unificado sin necesidad de un registro central. Los Identificadores Descentralizados (DID) brindan una convención de nombres similar a la de los Identificadores Únicos Universales (UUIDs). La diferencia reside en que los DID pueden ser resueltos como las URL o desreferenciarse a un recurso estándar que describa la entidad y, a diferencia de una URL clásica, normalmente contienen material cifrado, que habilita la autenticación de la entidad responsable del recurso (did:example:123456789abcdefghi). Según el *draft* del W3C, cada DID contiene al menos «material criptográfico, ”suites” de autenticación, y puntos finales de servicio». Un registro experimental DID que se ha establecido recientemente enumera una docena de proveedores de Blockchain, que incluyen BitCoin (did:btcr: did:stack:), Etherum (did:csnt, did:erc725, did:uport) y Sovrin (did:sov:).

Según Alexander Mayrhofer (nic.at), la contribución del DNS puede ser permitir un direccionamiento sencillo (y global), ya que las URL no son más fáciles de memorizar o de leer que un *hash* de blockchain. Gracias a la RFC 7553, la tecnología ya está lista, lo que permite «tipos de Registros de Recursos URI». La actualización de la RFC solo necesita agregar los DID

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

como un nuevo tipo (_did.example.net. IN URI 100 10 “did:sov:1234abcd”). Enlazar los DID a direcciones de email también es posible si un cliente solicita un registro DID en lugar de uno OPENPGPKEY (ver la sección 5 de la RFC 7929). Con respecto a la posible pérdida de privacidad/anonimato, Mayrhofer expresó que DID podría ser utilizado en algunas aplicaciones blockchain que necesitan poder ser encontradas y públicas. También observó que ofrecer la tecnología como basada en un estándar abierto evitaría la posible creación de soluciones propietarias.

El código en ejecución con un resolutor está disponible aquí.

Trabajos actuales en el DNS

Otro trabajo que se está realizando en el DNSOP es el de extender el uso del Tiempo de Vida (TTL) de un registro DNS «en la circunstancia excepcional en la que un resolutor recursivo no pueda actualizar la información». Al utilizar datos caducados, los cortes de un servidor pueden ser salvados. La propuesta de Warren Kumari (Google) fue bien recibida y ya es un documento del WG.

Charlas sobre la rotación de la KSK

Ahora habrá charlas con docenas de comunidades (esto no depende solamente de la comunidad del DNS) para decidir cómo proseguir con las futuras rotaciones. Se podrían debatir varias opciones, incluida la implementación en intervalos regulares —el director de tecnología de ICANN expresó hace poco que un intervalo de tres años sería un lapso razonable durante una entrevista para el blog de CENTR. A su vez, también se opinó que podría ser una buena opción tener una clave a largo plazo y una o varias claves de repuesto para implementaciones de emergencia.

Aún no existen estadísticas adecuadas. Los debates durante la reunión incluyeron los siguientes asuntos:

- Si debería haber una llave de repuesto en modo de suspensión (“standby”) (en una emergencia, la prepublicación no tendría sentido de todas formas), Wes Hardaker advirtió que especialmente para el software distribuido, podría ser beneficioso incluir la prepublicación y contar con varias llaves de reserva.
- Los cambios que se deberían efectuar en la RFC 5011 (rotación automática).
- Los cambios que se deberían efectuar en la RFC 8145 (la pregunta de Geoff Huston) para dar lugar a mejores mediciones (Señalizando el Conocimiento del Ancla de Confianza en las Extensiones de Seguridad del DNS).
- El momento en el que deberían considerarse rotaciones de algoritmos (¿se necesitaría más de una rotación completa de KSK antes de considerar una rotación de algoritmo?).
- ¿Cómo resultó la difusión de la rotación?

Geoff Huston advirtió que la rotación de la KSK no fue tan indolora como la describía ICANN. Encontró que hubo problemas en 75 redes (cuyo tamaño iba desde 25 a medio millón de hosts), y que posiblemente hasta cuatro millones de usuarios experimentaron problemas en total. Huston confirmó que el peor problema lo experimentó el proveedor de red irlandés EIR.com. De

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

acuerdo con sus cifras, en todos los casos excepto en tres instancias, las redes solucionaron los problemas por sí mismas. Tres redes simplemente dejaron de validar. Huston advirtió que en los resolutores más antiguos, los sistemas no podían ser atrapados por la telemetría utilizada. Hoffman reiteró que prácticamente nadie había ido a ICANN a quejarse o presentar problemas que hayan experimentado durante el proceso de rotación.

WG de TLS: ¿El final de la Extensión de la cadena DNSSEC?

Tras un acalorado debate, en su segunda sesión en Bangkok, el WG de TLS se movilizó para detener el trabajo sobre la propuesta de la extensión de la cadena DNSSEC, luego de que todos los representantes de las compañías de navegadores declararan que no la implementarían. Como consecuencia de la presentación que dio el copresidente de TLS, Sean Turner, sobre las continuas idas y venidas del trabajo del *draft* de la propuesta, el WG quitó el *draft* de la lista de documentos activos del WG. Turner admitió que no poder completar el documento reflejó que no estaban en «su mejor momento». Durante el debate, Wes Hardaker, a cargo del programa de mentores para los nuevos miembros del IETF, dijo que el 90% de las quejas sobre debates tóxicos hacían referencia al WG de TLS. La «naturaleza tóxica» del debate, según expresaron algunos participantes, hizo que dejaran de asistir a las discusiones relacionadas con el WG.

Última llamada y de regreso

Desde el IETF93, el WG de TLS ha trabajado en una "nueva extensión TLS para el transporte del conjunto de registros DNS serializados con firmas DNSSEC que se necesitan para autenticar ese conjunto de registros" (Extensión de la cadena DNSSEC). Los autores son Melinda Shore (Fastly), Richard Barnes (Mozilla), Simon Huque (SalesForge) y Willem Toorop (NI.net Labs). La idea de la propuesta, que tuvo un precedente elaborado por Adam Langley (Google) en 2012, era permitir que los clientes de TLS realicen una autenticación DANE de un servidor TLS sin realizar búsquedas DNS adicionales, evitando así problemas de latencia y de última milla de las DNSSEC.

Habiendo casi pasado la «última llamada del IETF» hace unos meses, surgió la preocupación sobre un posible ataque de versión inferior ("downgrade attack") cuando el IESG empezó a enviar comentarios. La preocupación, según Turner, es que «sin las listas blancas, un cliente dirigido erróneamente a un servidor que adquirió de manera fraudulenta un certificado emitido por una CA pública para el nombre del servidor real podría ser inducido a establecer una conexión con verificación PKIX al servidor comprometido que impida la autenticación DANE».

Los presidentes han intentado impulsar el documento para sobrepasar el último obstáculo varias veces. En el último debate, se intentó descifrar si dejar para luego el documento evacuaría las preocupaciones, y si los cambios en el foco ayudarían a terminarlo. Sin embargo, a esta altura parece que ya no se podrá llegar a un consenso en el WG. Durante el debate en Bangkok, algunos participantes hicieron comentarios duros sobre aquellos que todavía intentan arreglar problemas (incluidos Victor Dukhovni, de OpenSSL Foundation y autor de la RFC operacional de DANE, y Nicolas Williams, consultor en CryptoConnect). David Schinazi (Apple) no solo mencionó que Apple no aplicaría esto, sino que también pidió que le dieran un final al asunto

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

«porque está desperdiciando el tiempo del grupo de trabajo». Schinazi luego intentó dar un paso atrás, subrayando que todavía quedaban las RFC informativas.

Luego de que el WG quitó el documento del WG de TLS, queda por ver cómo reaccionarán los autores de las propuestas si intentan volver con un *draft* con cambios o publicar el documento como un documento individual.

Spin bit de QUIC: finalmente aceptado

Tras otra hora de debate, el WG de QUIC finalmente decidió que incluiría el spin bit en el Estándar QUIC, versión 1.0. El spin bit permite que los operadores de red (y otros) midan la latencia y solucionen problemas, según sus defensores. Con el spin bit establecido, el servidor y el cliente dan vuelta el bit cuando este los alcanza, lo que permite que el servidor mida los tiempos de recorrido.

Durante muchos meses, el WG había luchado en contra de agregar este bit extra, que fue solicitado por los operadores de red y algunas agencias de inteligencia (Centro de Ciberseguridad Nacional), porque QUIC cifra partes adicionales de los encabezados de transporte, lo que impide la utilización de metadatos para el monitoreo o la vigilancia del tráfico.

Se efectuaron varios cambios en la propuesta del spin bit para aliviar las preocupaciones sobre la vigilancia. En primer lugar, cada cliente y servidor tendrá la opción de decidir aplicarlo o no. Para evitar que aquellos que deciden no usarlo se distingan (y llamen la atención), los operadores deben asegurarse de que el spin bit no esté configurado en todas sus conexiones. Deben contar con una «configuración de anonimato».

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Uno de los problemas con estas medidas es que no queda claro si los operadores aplicarán la configuración de anonimato o no. Los representantes de compañías de navegadores (Google, Mozilla) y de plataformas (Facebook), junto con los proveedores Fastly y Protocol Labs, anunciaron que no implementarían el spin bit, por lo menos por ahora. Microsoft, Apple y Broadcom anunciaron que ellos lo implementarían. El spin bit sigue siendo una solución intermedia, según los expertos: con la solución de problemas y las mediciones de latencia, se podrían evitar o enfrentar los ataques, y los usuarios estarían más seguros. Al mismo tiempo, el bit extra brinda un poco más de información sobre un extremo de lo que es necesario.

El WG de QUIC se quedó atrás con respecto a su plan temporal original y sumamente ambicioso, pero la versión final de QUIC en la RFC debería estar terminada para principios del año próximo.

SUIT: ¿Uno o más formatos?

El grupo de trabajo de SUIT («actualizaciones de software para la Internet de las cosas») todavía está terminando sus documentos modelos de arquitectura e información, y se está atrasando un poco con respecto a los hitos establecidos. En Bangkok, el tema más importante que se abordó fue la pregunta de si el WG debería adoptar únicamente un formato de datos para el manifiesto, o si debería permitir varios, siempre y cuando utilicen el mismo modelo de datos[1].

Las diferencias entre los dos formatos que se presentaron en la reunión IETF103, una por parte de los desarrolladores de ARM, Brendon Moran y Hannes Tschofenig, y la otra por Martin Pagel de Microsoft, yacen principalmente en el protocolo que se utiliza para expresar el formato. Moran y Tschofenig proponen utilizar la Representación Concisa de Objetos Binarios (CBOR, por sus siglas en inglés), que supuestamente «ya está optimizada para tener un tamaño de código pequeño, mensaje pequeño, y extensibilidad sin la necesidad de negociar la versión». Pagel, en cambio, propone un formato binario txt simple, y brinda un panorama general de las diferencias entre estos dos candidatos.

Ventajas y desventajas del formato binario y la CBOR

«La CBOR facilita el manejo u omisión de campos opcionales o nuevos, mientras que una estructura binaria exige una estructura versionada para introducir nuevos campos, lo que complejiza su aplicación. Sin embargo, la estructura binaria tiene la ventaja de que se puede cargar en la memoria directamente, sin el uso de un analizador sintáctico. Por lo tanto, el código de instalación es mucho más simple o pequeño. Debido a que los instaladores son una fuente común de virus y vulnerabilidades, se considera que un código simple es, por lo general, más seguro. Aborda muy bien la Sección 3.6/7 del documento de arquitectura (pequeño gestor de arranque (“bootloader”) y analizador sintáctico (“parser”)). Además, la separación de URIs de imágenes da lugar a un manifiesto mucho más pequeño y, por lo tanto, reduce las exigencias de la memoria. Puede que un dispositivo básico no pueda ser compatible con muchas opciones de todos modos, y estos dispositivos tienen más restricciones de espacio; el formato binario puede

[1] Los manifiestos son «un conjunto de metadatos sobre el firmware de un dispositivo IoT: dónde encontrar el firmware, los dispositivos a los que aplica, y la información de cifrado que protege los datos del manifiesto».

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

ser una mejor opción. Un dispositivo más sofisticado puede ofrecer más opciones y usar la CBOR con otros propósitos y, así, puede que este formato propuesto sea más adecuado».

La opinión preliminar formada por el WG mostró que la mayoría prefiere que la cantidad de formatos de datos sea solo uno, lo cual representa un objetivo ambicioso. Al mismo tiempo, casi la misma cantidad de participantes indicó que «se necesita más información». Por lo tanto, continuarán los debates. Existió una tercera propuesta por parte del Instituto Fraunhofer SIT que no se presentó ni debatió en Bangkok.

Gurshabad Grover, del RG de HRPC, preguntó si esto era suficiente para hacer seguro el camino: el debate sobre la seguridad adicional para los datos fue infructuoso.

Otra cuestión debatida en el WG fue el vínculo entre la IoT y la UIT. El WG acordó mantener la coherencia terminológica tanto como sea posible entre SUIT y SG17, que está actualmente terminando su propio documento sobre IoT.

Mientras tanto, y en relación con el trabajo sobre la IoT, CIRA está llevando a cabo su proyecto de estandarización de portal seguro, pero parece estar en busca del lugar y el grupo de trabajo adecuados en el IETF.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Grupos de investigación

¿El RG de SMART es una buena idea?

Tras perder la batalla para tener una clave estática para el nuevo TLS 1.3 (ver el Informe IETF101), las agencias de aplicación de la ley y varias compañías intentaron recuperar terreno perdido. A modo de ejemplo, el Centro de Ciberseguridad Nacional de Reino Unido (NCSC, por sus siglas en inglés) tomó una iniciativa para formar un grupo de investigación dedicado a descubrir cómo se pueden detectar amenazas en el tráfico cifrado. El *draft* de la carta constitutiva del RG de SMART reza: «El grupo de investigación de Detención de Malware e Investigación de Amenazas (SMART, por sus siglas en inglés) investigará cómo se pueden satisfacer los requisitos de defensa contra ciberataques en un mundo de datos cifrados».

Durante una reunión paralela (un nuevo formato de sesión en la reunión IETF103) presidida por Kirsty Paine (NCSC) y la exdirectora del Área de Seguridad, Kathleen Moriarty (Dell), Paine subrayó que el grupo de trabajo no estaba destinado, bajo ningún punto de vista, a debilitar los nuevos estándares de seguridad desarrollados en el IETF, incluido el cifrado. Sin embargo, el grupo de investigación fue creado para «investigar los efectos, tanto negativos como positivos, de los protocolos existentes, propuestos y recientemente publicados y de los estándares de Internet sobre la defensa contra ataques».

Los ataques pueden ser malware, *phishing*, ataques DDoS y también, como dijo Moriarty, el monitoreo dominante. Durante la sesión, Paine enumeró algunos de los temas por investigar: las capacidades y limitaciones de la detección en el extremo, la detección de amenazas en el tráfico cifrado, y las métricas para lo bueno y lo malo.

Los miembros del grupo de investigación, incluidas las agencias de aplicación de la ley y de inteligencia, pueden presentar información sobre casos para ejemplificar los problemas, y el RG puede hacer comentarios sobre los estándares en desarrollo, ofrecer alternativas para llegar a niveles más altos de defensa frente a ataques, e incluso proponer soluciones. Según el *draft* de la Carta constitutiva, «Durante el primer año, los objetivos del grupo de investigación serán los siguientes:

- Examinar los métodos existentes para la detección de ataques y determinar la eficacia relativa de estos frente a diferentes amenazas hacia la defensa contra ataques (por ejemplo, *phishing*, ataques DDoS, spambots, ataques de comando y control [C&C], y malware en el extremo).
- Publicar casos prácticos de ataques históricos y determinar dónde se podría haber detenido el ataque con mayor rapidez, o incluso si se podría haber evitado.
- Publicar una RFC Informativa, con el siguiente título: “Consideraciones importantes sobre la defensa contra ataques en el diseño y desarrollo de protocolos”».

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

¿Consideraciones sobre la defensa contra ataques?

La RFC «Consideraciones importantes sobre la defensa contra ataques en el diseño y desarrollo de protocolos» prácticamente imita la RFC 8280 (y el correspondiente documento de directrices en consideración), y parece que hay expectativas de que las agencias de aplicación de la ley y de defensa puedan también dar sus consejos.

Paine también recalcó que no era su intención superponerse al trabajo del Área de Seguridad en lo que respecta al asesoramiento brindado a los WG sobre los posibles riesgos y problemas de seguridad. Sin embargo, uno podría preguntarse si el grupo decidió que necesitaba mejorar su desempeño en cuanto a las consideraciones de aplicación de la ley (¿seguridad pública?), debido a los trabajos previos en materia de seguridad, privacidad y derechos humanos.

Las reacciones de los participantes durante la atestada reunión paralela (entre 25 y 30 asistentes) fueron diversas. El exdirector de Área de Seguridad Stephen Farrell recomendó que la carta constitutiva no fuera demasiado ambiciosa, pero, al mismo tiempo, que deberían llegar a resultados concretos rápidamente.

Bret Jordan, de la Dirección de Tecnología de Symantec, aplaudió la iniciativa y expresó que el grupo llenaría un gran vacío en el IETF y que «si el marketing se hace de la manera correcta, habrá muchas personas».

Se espera que la primera reunión oficial del RG sea en Praga (IETF104). El grupo también enviará un llamado a presentaciones para el segundo taller de CARIS (Coordinación de respuestas a ataques a escala Internet) en las próximas dos semanas.

Búsqueda del foro más conveniente para la estandarización: ¿un ataque al TLS?

Desde que finalizó la reunión IETF103, la lista de mails del grupo ha estado en silencio, a excepción de un comentario de Daniel Kahn Gillmore (ACLU) sobre la investigación que analiza los riesgos del seguimiento de usuarios a través de la reanudación de TLS (evitando los viajes de ida y vuelta al reanudar las sesiones TLS con los hosts que ya han sido visitados).

Sin embargo, puede que existan discrepancias en la búsqueda de un foro favorable, ya que varios publicaron una versión que usa claves estáticas para romper el concepto de extremo a extremo y permitir la interceptación. Mientras tanto, el IETF le pidió al ETSI, el organismo de estandarización en cuestión, que desista en absoluto de llamar eTLS al TLS. El organismo europeo de estandarización ETSI acaba de anunciar su variante del TLS 1.3 (TLS empresarial, que antes era TLS de contexto múltiple) para el TLS empresarial (eTLS) que permitirá a los administradores de centros de datos mantener el control de las claves TLS para los puntos extremos (como mínimo). La razón de ser de la propuesta del ETSI es, principalmente, quebrar el nuevo TLS 1.3:

«Existen requisitos —como los mandatos legales y los contratos de servicios— para que las operadoras de redes y centros de datos empresariales y los proveedores de servicios, organizaciones, y pequeños comercios puedan observar y auditar el contenido y los metadatos

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

de sesiones cifradas transportadas en sus infraestructuras [i.2]. El estándar del protocolo TLS original que se adoptó en 1994 y sus versiones siguientes, incluida la TLS 1.2, contemplaron estas capacidades [i.3] y [1]. La versión más reciente del protocolo (TLS 1.3) no contempla estas capacidades [2]. Donde no existan estas capacidades, el nuevo protocolo de cifrado se podría bloquear completamente en el portal corporativo, lo que obligaría a los usuarios a volver a usar protocolos más antiguos y menos seguros. El presente documento forma parte de una serie de perfiles de implementación que, para lograr las capacidades exigidas, les cede a los operadores empresariales y a los usuarios el control del acceso a sus datos para la ciberdefensa y evita el acceso no autorizado. Establece un "Perfil para el control de acceso de una red y centro de datos empresariales" llamado eTLS, que cumple con varias capacidades deseadas para el Protocolo de Seguridad de *Middlebox* (MSP) [i.1]».

Básicamente, con la implementación del eTLS, el TLS 1.3 se termina en el cortafuegos de la red. Luego, el cortafuegos o el servidor web interno actúa como cliente de TLS 1.3 entre el cliente de la red y la aplicación externa o entre el cliente externo y la aplicación dentro de la red.

EXAMPLE 2: Middlebox B decrypts the traffic in real-time to provide application health monitoring, but also stores the encrypted packets so they can be decrypted at a later date for compliance and auditing purposes.

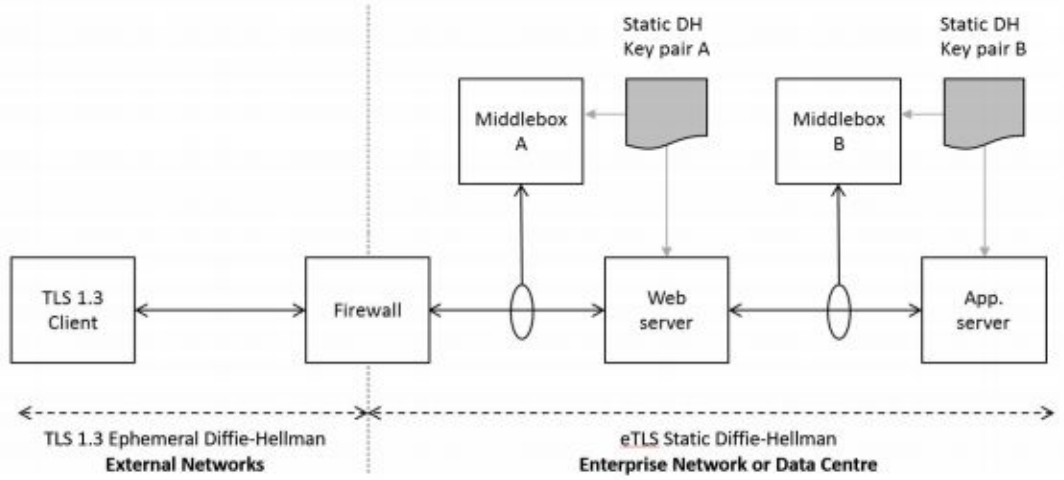


Figure 4.1: eTLS architecture with enterprise servers

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

4.2.2 eTLS with enterprise clients

Figure 4.2 depicts the eTLS implementation architecture when used with enterprise clients. TLS connections to servers that are external to an enterprise network may be made using TLS 1.3 [2], using forward secrecy and enhanced protections.

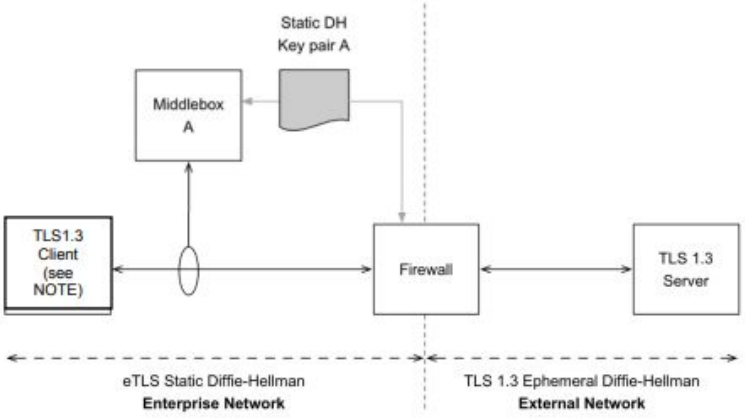


Figure 4.2: eTLS architecture with enterprise clients

Esta propuesta, en esencia, retoma lo que se discutió durante la sesión del WG del TLS en el IETF, pero que nunca llegó a un consenso. A su vez, limita la visibilidad. Los clientes que no hayan implementado la visibilidad de eTLS no sabrán que las *middleboxes* que descifran el tráfico están involucradas, y que naturalmente, tampoco «recibirán, si se solicita, la validación de identidad de cada *middlebox*».

Lo que sigue siendo un interrogante es cómo reaccionará el IETF a la búsqueda del foro más favorable sobre el TLS, por el cual reclama DPI y control de cambios. Si bien el Comité Técnico de Ciberseguridad (TC Cyber) del ETSI prometió «no usar el nombre TLS si no se refiere a los estándares del IETF» en una carta, el documento publicado se refiere claramente al nuevo estándar del ETSI como una «variante de implementación» del TLS. El ETSI también hace referencia a estándares similares al permitir el descifrado de *middleboxes* en la UIT.

Además de esto, el ETSI desafía el hecho de que el IETF pueda reclamar derechos de autor sobre el TLS y menciona tecnología relacionada que, según el ETSI, es anterior al conjunto de estándares de TLS del IETF. El Área de Seguridad del IETF rechazó esta afirmación es su declaración de cooperación el 5 de diciembre.

El IETF ha perdido batallas anteriores sobre el protocolo de transporte MPLS, y la aplicación de la ley de la UE ha usado anteriormente al ETSI en eventos de elección de estándares, en especial con respecto a la Intercepción Lícita (LI) de las redes de comunicación.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Grupo de investigación cuántica

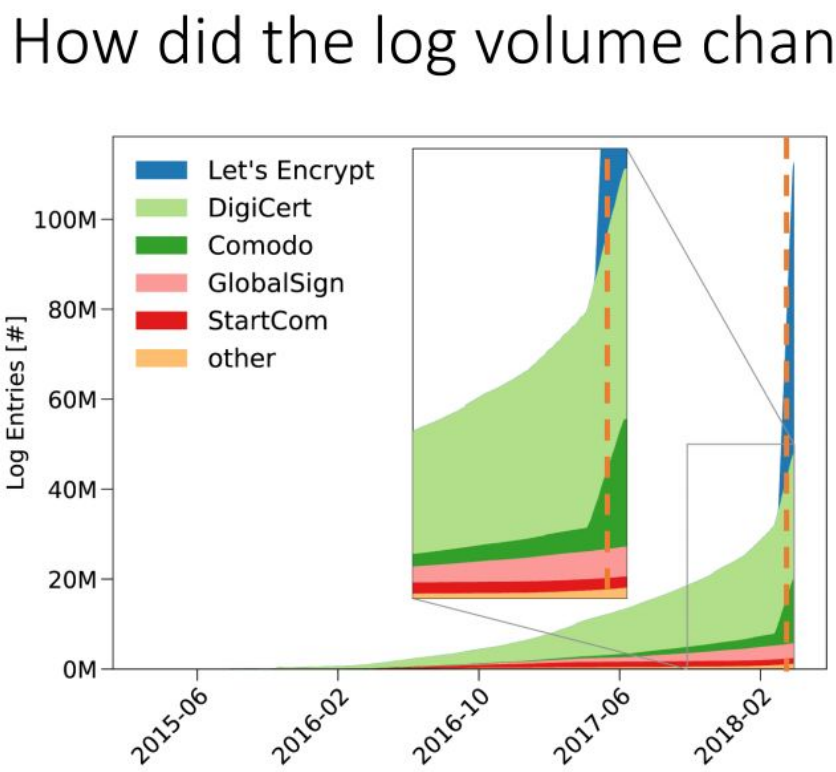
El IRTF está por formular la carta constitutiva para el Grupo de investigación cuántica que, como el nuevo RG de SMART, se reunirá oficialmente por primera vez en la reunión IETF104 en Praga. En una sesión preparatoria con una buena convocatoria (100 asistentes), quien impulsó el RG y su futuro copresidente, Rod van Meter (Universidad Keio) explicó la razón de ser del grupo de investigación. Si bien el trabajo sobre la Internet Cuántica está bien encaminado, los físicos que trabajan en el entrecruzamiento y el intercambio de claves carecen de conocimientos sobre ingeniería de la red. Asimismo, los investigadores de física cuántica reconocen que, en lo que respecta a las aplicaciones, necesitan avanzar con la decisión sobre «qué haríamos con una Internet Cuántica» y cómo desarrollar un sistema multipartidista (en lugar de los sistemas simples de transferencia de punto a punto que están en desarrollo actualmente). La otra copresidenta, Stephanie Wehner (TU Delft), y otros dos colegas describieron una visión del camino para las redes cuánticas aquí. El RG espera convertirse en el foco de la estandarización de las redes cuánticas y también espera consultar al IETF sobre el cifrado cuántico.

Según la carta constitutiva propuesta, el grupo de investigación trabajará en lo siguiente:

- **Enrutamiento**: ha habido varias propuestas, un par de ellas en estos últimos seis meses. Por lo tanto, será necesario evaluar cuáles esquemas de enrutamiento serán los apropiados en las distintas circunstancias.
- **Asignación de recursos**: parece que algunas propuestas de enrutamiento incluyen una noción del tráfico dinámico en la red, pero esta distinción debe estar claramente definida.
- **Establecimiento de la conexión**: ¿cómo se ve una solicitud (en cuanto a semántica más que sintaxis) a medida que se propaga en la red?
- **Interoperabilidad**: dado que, actualmente, se están diseñando y construyendo diferentes redes, ¿cómo aseguramos el desarrollo de una red duradera?
- **Seguridad**: ¿las redes repetidoras cuánticas son inherentemente más o menos vulnerables en las operaciones que las redes clásicas?
- **Diseño de una API**: una API que cumpla el rol de los puntos de conexión de las redes clásicas.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Transparencia de certificados



En dos presentaciones muy interesantes (durante la reunión abierta del IRTF y el RG de MAP), los investigadores Johanna Aman (ICSI California) y Matthias Wählisch (Universidad de Hamburgo) presentaron las estadísticas sobre la evolución del TLS y la transparencia de certificados (CT), ilustrando las implicancias de exponer los nombres de DNS certificados desde la perspectiva de la seguridad y la privacidad. Aunque descubrieron que se había asentado un exponencial crecimiento de certificados en los registros de transparencia, y que el soporte web para la CT representa un 33% de las conexiones establecidas, también encontraron que tomó solo una hora antes de que estuvieran las primeras búsquedas DNS para los dominios que habían establecido con los certificados en la lista. En la mayoría de los casos, los investigadores no pudieron averiguar quién los había escaneado (no había información en el rDNS, WHOIS ni en el sitio web). Un escáner solicitó registros rápidos A/AAAA y escaneó 30 puertos. Si bien la transparencia de certificados ayuda a encontrar atacantes de *phishing*, la filtración de información sigue siendo un problema. Los investigadores también descubrieron que solo unos pocos registros conservaban todas las entradas al registro.

También se expresaron sobre la privacidad añadida a través del cifrado. Consideran que dañan sus mediciones, pero piensan que, a fin de cuentas, el cifrado añadido es la mejor opción.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

El HRPC lucha contra sus propios procedimientos

Además de las continuas charlas sobre cómo debería proceder con su trabajo el HRPC, la copresidenta Avri Doria advirtió que el grupo no debe actuar como si fuera una «Dirección» propiamente dicha del IETF, ya que no lo era (el grupo había invitado a Arthit Suriyawongkul de la Thai Netizen Network para hablar sobre la libertad de asociación y tecnología. La Thai Netizen Network monitorea la acción legislativa actual en su país, específicamente la legislación sobre protección de datos (que da lugar a muchas exenciones a la seguridad nacional, la policía, las compañías de seguros, etc.) y la legislación en materia de ciberseguridad.

Según Suriyawongkul, un problema desde el punto de vista de la ONG es que, a menudo, la seguridad percibida no concuerda con la seguridad real que ofrecen los protocolos. En su presentación, habló sobre el derecho de asociación en línea, y lo relacionó tanto con la libertad de expresión (básica, individual) como con la privacidad (indispensable para ejercer otros derechos), y también indicó nuevas maneras en las que se puede atacar a los detractores. En varios países, la policía ha comenzado a reproducir música protegida por derechos de autor durante las protestas, lo que ha resultado en la eliminación de las marchas (y discursos) de protesta transmitidas desde YouTube por razones de derechos de autor.

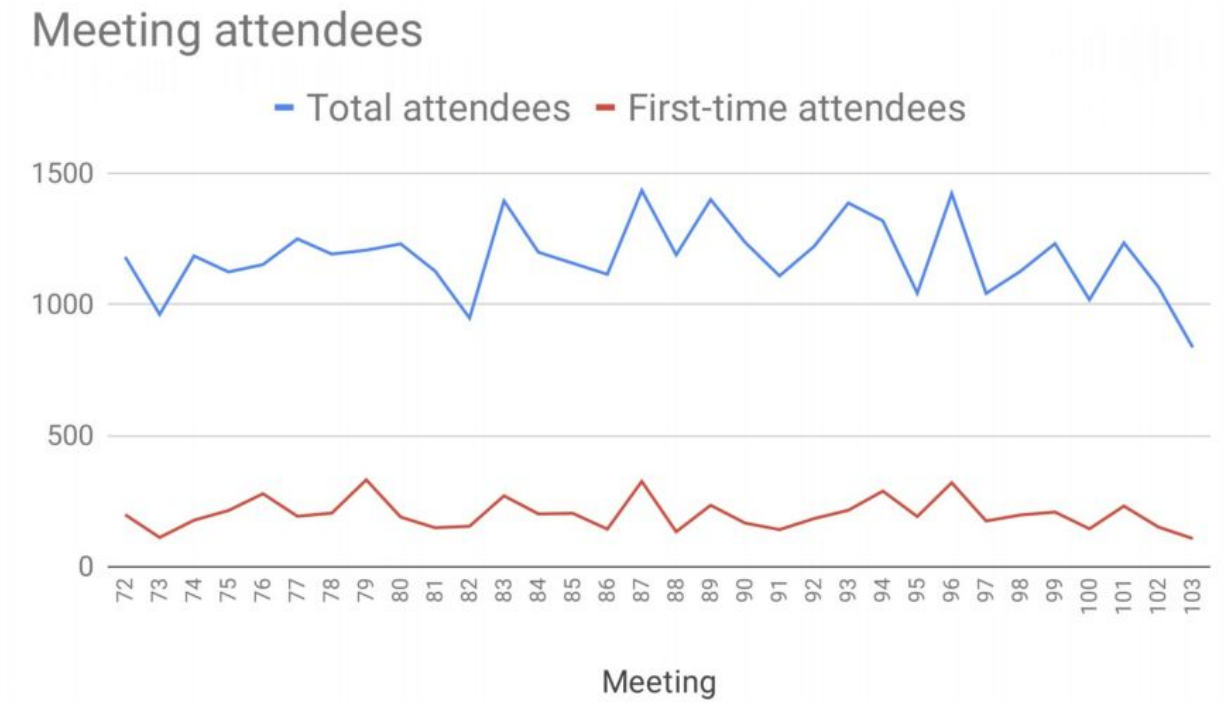
¿Un caballo de Troya en el HRPC?

Llegó al grupo de HRPC una propuesta de Nalini Elkins (Enterprise Data Center Operators), la cual es poco precisa, sobre cómo debería perfeccionarse el filtrado mediante el uso de protocolos del IETF, con base en el concepto de que el IETF no debería seleccionar minuciosamente los derechos, sino defender todos los derechos humanos. Si bien Elkins se centró en varios ejemplos de filtrado y fundamentos en el *draft*, durante la charla intentó explicar por qué el filtrado era necesario para evitar pérdidas humanas. Argumentó que el derecho humano a la vida entra en conflicto con el derecho a la libertad de expresión y a la privacidad. Elkins está entre quienes piden una clave estática en el TLS 1.3. Durante la sesión, la presidenta del RG, Avri Doria, señaló que el «*draft* de filtrado» debería concentrarse en la descripción del panorama del filtrado y no en convertirse en un *draft* operacional.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Noticias del IETF

La participación en Bangkok fue muy baja: contó con apenas 850 participantes, aproximadamente. La presidenta del IETF, Alissa Cooper, quien presentó las estadísticas, expresó que este era un altibajo natural.



De los diferentes experimentos para atraer más participantes, la hackatón parece ser la opción más prometedora. Cooper informó que había muchas personas que viajaban al IETF exclusivamente para asistir a la hackatón.

Sin mucha ostentación, el IETF estableció su organización LLC, que fue creada legalmente el 27 de agosto de 2018, y que asumió las responsabilidades del IAOC. El director ejecutivo del IETF remplaza el puesto de IAD, y al puesto lo ocupará el Comité de Nominaciones, con Portia Wenze-Danley, que actualmente se desempeña como directora ejecutiva interina. La junta directiva de la LLC del IETF, compuesta por cinco directores (uno elegido por el IESG, otro por el Consejo de Administración de la ISOC, y tres por el Comité de Nominaciones) asumirá el rol del IAOC. Se anunciará cómo se compone la junta directiva en la reunión IETF104. La junta directiva interina actual está compuesta por Glenn Deen, presidente del IAOC (presidente de la LLC), Alissa Cooper (presidenta del IESG), Ted Hardie (presidente de la IAB) y Gonzalo Camarillo (presidente del Consejo de Administración de la ISOC).

La IAB y las plenarias técnicas

El viernes abierto para el experimento de reuniones paralelas que no sean de los grupos de trabajo no funcionó por completo, ya que muchos organizadores de las reuniones paralelas decidieron llevar a cabo reuniones paralelas antes del viernes. Andrew Sullivan, presidente de la

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

ISOC, también se quejó porque las sesiones plenarias técnicas casi debieron abandonarse. No obstante, como señaló Sullivan, las plenarias técnicas le permitían a la comunidad del IETF mantener charlas intergrupales sobre desarrollos técnicos actuales interesantes. El comité del programa para las plenarias técnicas está buscando más personas, pero mantendrá plenarias técnicas nuevamente en el futuro, según el presidente de la IAB, Ted Hardie.

La IAB publicó varios informes sobre talleres que tuvieron lugar hace años (la RFC 8477, un informe del taller de Interoperabilidad Semántica [IOTSI] de la Internet de las Cosas [IoT] y la RFC 8462, un informe del taller de la IAB sobre el Manejo de Redes Radiales en un Mundo Cifrado [MaRNEW]). Ahora existe un nuevo debate sobre cómo lidiar con la presentación de informes. Con respecto a la transparencia, la IAB respondió a las quejas y ha abierto sus reuniones a observadores. Asimismo, ahora se publicarán las agendas de las teleconferencias de la IAB. La carta de la IAB remitida al legislador australiano es una buena lectura en lo que respecta a sus ocasionales declaraciones políticas en relación con que Australia propuso un proyecto de ley de Asistencia y Acceso (que romperá el cifrado).

Nuevos nombramientos

Tim Wicinski – Grupo de Coordinación de la Comunidad (asesoramiento para la Fundación IETF)

Ole Jacobsen – renombramiento por parte del Comité de Nominaciones de ICANN

Sarah Banks, Tony Hansen, Adam Roach, Peter Sant-Andre, Robert Sparks, Christian Huitema – miembros del Comité de Supervisión de Series RFC

Próximas convocatorias:

La IAB está en la búsqueda de un nuevo presidente para el IRTF, ya que Alison Mankin concluirá su mandato el año próximo.

Voluntarios para el Grupo de Cooperación Técnica de ICANN.

Consejo de Administración de la ISOC.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22