Informe sobre IETF 107

Reunión virtual, del 23 al 27 de marzo de 2020

El informe fue producido por CENTR y traducido por LACTLD

Agradecemos 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

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

Contenidos

Reunirse virtualmente no es fácil

La cancelación con poco preaviso de la reunión presencial del IETF recibió, inicialmente, algunos comentarios críticos. Sin embargo, dado que la cantidad de casos de COVID-19 se duplicó durante la semana del IETF, dichas críticas no duraron mucho.

Lo que funcionó

La presidenta del IETF, Alissa Cooper, informó que unas 701 personas de 39 países diferentes participaron en las sesiones virtuales, con "cifras de entre 82 y 235 participantes en cada sesión de trabajo y 282 personas que se unieron a la sesión plenaria".

El equipo directivo de la reunión IETF 107 había asignado dos o tres lugares de reunión al día para nuevos grupos de trabajo (WG), y a los grupos de trabajo existentes les delegó la organización de sus propias reuniones interinas virtuales. Es probable que algunas de las reuniones informales (BoF) hayan tenido una mayor participación de la que tendrían en una reunión normal.

Desde la perspectiva técnica, el auspicio de Cisco permitió que el IETF use Webex para la reunión. A grandes rasgos, funcionó bien, pero debido a que la función de chat en Webex se usó para gestionar las filas, los participantes informaron un mayor uso de los chats de Jabber durante las sesiones en las charlas posteriores de la lista de correo electrónico de los asistentes.

Lo que no funcionó tan bien

Los debates paralelos en Webex y Jabber no permitieron que los presidentes de los WG perciban el ambiente de la reunión de la manera en que lo hacen habitualmente. Aun así, los escribas de las minutas y Jabber prometieron hacer el intento de incluir los comentarios relevantes de ambas conversaciones en las minutas de las reuniones.

Algunas de las sesiones se abreviaron y generalizaron bastante. Las BoF no prosiguieron con las típicas preguntas de BoF, y el intercambio general de opiniones parece ser más difícil en línea. El WG de Adaptive DNS Discovery (ADD) sirve de ejemplo de que el formato virtual no se prestó para fomentar los debates sobre cómo seguir adelante (vea a continuación).

Desde el punto de vista organizacional, la reunión en línea hizo más difícil notar las reuniones paralelas emergentes. Algunas reuniones paralelas individuales, por ejemplo, se llevaron a cabo sin estar incluidas en la agenda virtual oficial; en específico, la reunión paralela sobre el "Nuevo IP" (vea el gráfico sobre este tema candente más abajo).

Las grabaciones de todas las sesiones oficiales están disponibles en el sitio web y en el canal de YouTube del IETF.

El futuro en línea en tiempos de coronavirus

La reunión de RIPE en mayo será en línea únicamente (y quizás dure solo un día), y se espera que la próxima reunión del IETF en julio también se convierta en una reunión en línea, con posibles cambios de formato.

En su posteo de blog sobre la reunión IETF 107, Cooper escribió que, por ahora: "El IESG y el IETF LLC están trabajando en conjunto para planificar las próximas reuniones en vista de la actual pandemia". Algo que se debatirá sin dudas será qué hará el IETF para gestionar los costos de la participación remota en el futuro, especialmente cuando haya que poner en línea más reuniones. Mientras tanto, Cooper anunció que la decisión sobre la reunión de julio se tomará para el 15 de mayo de 2020.

Varias de las reuniones de WG habituales, como las de DPRIVE y DNSOP, que fueron relegadas para dar lugar a las reuniones de nuevos WG y BoF (para permitir que se organizaran y comenzaran a trabajar), se llevarán a cabo durante las próximas semanas. Puede encontrar la agenda aquí.

VoIP a la web: el encanto de HTTP

Con la transición del DNS al protocolo web HTTPS, los ingenieros del IETF están pensando en otra transición web. Se trata de una propuesta de reemplazar el viejo protocolo SIP para Voz sobre IP por el protocolo Peering de Internet en Tiempo Real para Telefonía (RIPT) y, finalmente, incorporar la telefonía a la red.

Según el autor del *draft* sobre RIPT, Jonathan Rosenberg, el SIP era "un desastre", debido a las *middleboxes* como los balanceadores de carga que interrumpen las conexiones. El SIP no fue diseñado para funcionar con direcciones IP asignadas de manera dinámica, aunque la traducción de direcciones de la red se ha convertido en una nueva norma de Internet.

Rosenberg fue uno de los autores del estándar original del SIP, la RFC 2543, publicada en 1999. En la reunión IETF 107, presentó las nuevas ideas de especificación de VoIP durante la BoF de RIPT. "Queremos que VoIP use la web", dijo, y enumeró las eficiencias de los balanceadores de cargas, las actualizaciones sin impacto, mallas de servicios, y georredundancia.

El "encanto del ecosistema de HTTP", según escribió Patrick McManus de Fastly a quien escribe en un intercambio de correos electrónicos, es "muy fuerte, porque aporta distintas tecnologías de seguridad y escalamiento de carga, y continúa evolucionando".

El camino hacia HTTP3

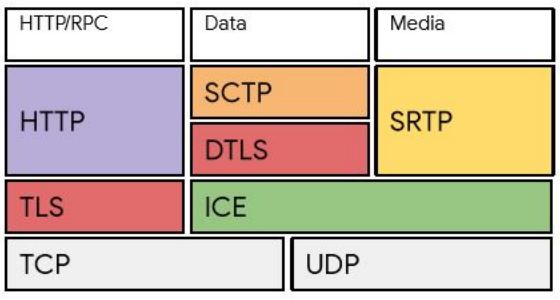
Según la propuesta de Rosenberg, RIPT sería optimizado para la versión más reciente de HTTP, HTTP3, con su seguridad agregada (TLS por defecto) y capacidades de multiplexación. Sin embargo, un futuro estándar deberá establecer mecanismos de respaldo, considerando que muchas aplicaciones aún no usan ni siquiera HTTP2.

Otra cuestión interesante para el WG de RIPT será la comunicación mediante video y audio entre pares (P2P). Los modelos de seguridad de HTTP hacen imposible el P2P, tal como observó el expresidente del IETF y exdesarrollador de Google, Harald Alvestrand, ya que la seguridad de HTTP exige la verificación de identidad del servidor. También se debatió sobre el cifrado de extremo a extremo, el manejo de claves y el spam de llamadas.

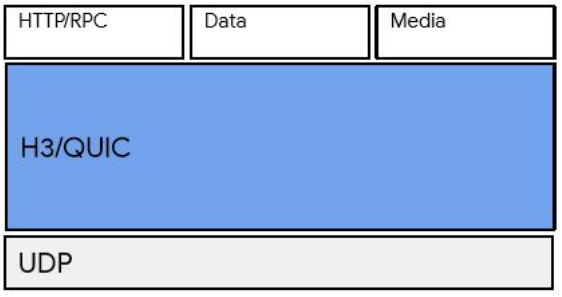
¿Cuáles serán las especificaciones?

“Usaremos RIPT si esto sale bien”, dijo Anthony Minnesale de SignalWire. Desde hace 15 años, su empresa desarrolla software de la pila de telecomunicaciones de código abierto (FreeSwitch). Otro usuario interesado es Google, según Justin Uberti, considerando pasar de la actual pila compleja WebRTC a la pila de HTTP basada en transporte QUIC, que es mucho más sencilla (vea los gráficos más abajo).

Parecería que la fuerza conjunta de los defensores de un nuevo estándar debería poner un freno a las preocupaciones de que una futura RFC del IETF tendría un solo gran usuario del estándar. La expectativa parece ser que el VoIP web será interesante para muchos, dependiendo, por supuesto, de cómo sea cuando esté terminado.



WebRTC



Para obtener más información, consulte los siguientes *drafts*:

https://tools.ietf.org/html/draft-rosenbergjennings-dispatch-ript-00
https://tools.ietf.org/html/draft-rosenberg-dispatch-ript-inbound-00
https://tools.ietf.org/html/draft-rosenberg-dispatch-ript-sipdiffs-00
https://tools.ietf.org/html/draft-rosenberg-dispatch-ript-webrtc-00

O vea las notas de Etherpad sobre la BoF de RIPT en el siguiente enlace:

https://etherpad.ietf.org:9009/p/notes-ietf-107-ript?useMonospaceFont=true

¿Quo vadis, DNS: DoT, DoH, DoQ?

La primera reunión del WG de Adaptive DNS Discovery (ADD) del IETF no fue concluyente. Si bien hay un amplio consenso en que tanto los proveedores de DNS como los clientes o los usuarios necesitan contar con opciones de resolutor, parece que el WG se verá superado por otro contrincante de resolución de DNS cifrado en DNS sobre QUIC (DoQ).

Los participantes escucharon tres opciones para el descubrimiento de servidores DNS recursivos, pero ninguna recibió respaldo suficiente para ser elegida como el paso siguiente.

DoT y DoH con descubrimiento local, por favor

La propuesta presentada por Dan Wing ante un grupo de autores que incluyó a Orange, Citrix, Open Exchange y McAfee, ofrece la selección de servidores DoH y DoT para redes fijas y móviles, preferentemente en la red local mediante un nuevo identificador de referencia de DHCP (y DHCP6) (DoT) y opciones o listas especiales para DHCP/RA (DoH). La propuesta pone énfasis en las ventajas de mantener resolutores de manera local para un mejor desempeño, haciendo alusión al tráfico 5G.

Comparada con las otras opciones, esta serie de *drafts* ofrece transparencia al usuario con respecto a las propiedades de privacidad, según Alexander Mayrhofer, experto en DNS en nic.at. “Estamos trabajando para priorizar la privacidad, por lo que comunicar estas propiedades parece una buena idea”, dijo Mayrhofer, “incluso si no sabemos si se puede lograr la ‘decisión informada’ como tal”.

¿Una lista de resolutores en la IANA?

La propuesta sobre un “Protocolo de Descubrimiento de Resolutores DNS” (DRDP) del ingeniero de Ericsson, Daniel Migault, recibió muchas críticas. El *draft* considera el descubrimiento de recursivos mediante una lista gestionada por la IANA u otro foro especial. Como se espera que la cantidad de resolutores públicos globales compatibles con DoH y DoT sea baja, Migault recomienda que deberían ser recuperables mediante un dominio especial: rdns.arpa.

Tras la reunión, Migault se dirigió a las críticas y estuvo de acuerdo en que, en lugar de tener un lugar central para la consulta de resolutores públicos, sería mejor contar con "repositorios" descentralizados en la medida de lo posible.

¿Usar HTTP para reconstruir el árbol DNS?

Algunas caras conocidas del ambiente HTTPS, Tommy Pauly de Apple y Patrick McManus de Fastly, hicieron una propuesta diferente pero similar ante el WG de DPRIVE, que sugiere que el descubrimiento debería estar basado en solicitudes HTTP. Los resolutores serían encontrados recursionando desde un autoritativo/resolutor DNS conocido (para el *bootstrapping*). Esto se combinaría con otro *draft* de privacidad del DNS: "Oblivious DNS", en el que el autoritativo/resolutor podría actuar como proxy.

La característica importante de "Adaptive DNS", según McManus, era un "menor énfasis en los resolutores recursivos terceros: por lo tanto, haría un mejor trabajo al compartir la información del nombre con solo aquellos que estén involucrados en la transacción HTTPS". McManus opina que el flujo de datos era "similar a aquel de un *stub* que implementa su propio recursivo", pero con mejores propiedades de seguridad. La propuesta de Adaptive DNS tiene sus fans, entre los que se incluyen algunos expertos en DNS. Sin embargo, la mayoría piensa que se necesita mucho más despliegue de DNSSEC para evitar el *bootstrapping* desde un resolutor falso, aunque McManus piense que HTTPS puede realizar también la tarea.

El turno de DoQ

Mientras el grupo de ADD sigue organizándose, el WG de DPRIVE considerará otro *draft*, DNS sobre QUIC (DoQ), en su reunión virtual del 8 de abril de 2020.

Algunos opinan que QUIC, el nuevo protocolo de transporte que se prevé completar en 2020, podría terminar representando una porción considerable del futuro tráfico de Internet. Debido a que está basado en el UDP pero, a la vez, promete aportar eficiencia poniéndole fin al bloqueo de cabeza de línea e incorporando el cifrado por defecto, puede que encaje muy bien con el DNS. Al menos eso es lo que piensan los autores y gurús de la privacidad, Christian Huitema, exmiembro de la IAB, Sara Dickinson, de Sinodun, y Allison Mankin de Salesforce.

El DoQ dependerá de que QUIC se implemente de manera más amplia, mientras que no se espera que la implementación de HTTP3 sea un requisito previo. Por el momento, los autores limitan el DoQ a la ruta del *stub* al recursivo. Además, los autores escribieron que el riesgo de que las *middleboxes* bloqueen las conexiones de QUIC no se puede abordar.

Tomando una decisión

Cuando haya suficiente apoyo de los navegadores para QUIC y HTTP3 y el HTTP basado en TCP sea "obsoleto", el DoQ podría volverse mucho más atractivo en comparación con el DoH para las solicitudes a nivel de aplicación, según Mayrhofer.

Para el software DNS existente, adaptarse al DoT sigue siendo la opción más sencilla, aunque tenga problemas con el filtrado y el bloqueo mediante firewalls debido a su número de puerto especial, según comentó Mayrhofer. Por lo tanto, para todo despliegue de infraestructura (incluso la futura ruta de servidor recursivo a autoritativo), sigue siendo una opción atractiva. Mayrhofer describe la actitud de partes del ambiente del DNS con la frase "¿Por qué se añadiría una pila HTTP aquí?". Peter Koch de DENIC es, por ejemplo, uno de los que cuestiona el valor de una recreación del árbol DNS en HTTPS. No obstante, los beneficios de seguridad y escalamiento de carga seguirán siendo la respuesta de los proveedores de navegadores y de sistemas operativos móviles.

Ni Mayrhofer ni Huitema creen que se aplacarán las discusiones entre las comunidades del DNS y de la web, por lo menos por el momento.

Gestionando ventajas y desventajas

En un gran intento final de estructurar el trabajo del WG de ADD, el presidente saliente de la IAB, Ted Hardie, se unió a sus colegas de la IAB Jari Arkko y Martin Thomson para presentar una propuesta sobre transparencia de privacidad para diferentes procedimientos de descubrimiento de resolutor. La idea de este *draft* es visibilizar los procesos de toma de decisiones y las ventajas y desventajas a las que se enfrenta la comunidad IETF ante partes externas, como los consumidores finales y los usuarios.

Una de las observaciones clave es que, si se permitiera el descubrimiento de múltiples resolutores DNS, se abriría camino a futuras reducciones en la concentración de la información sobre la actividad de un cliente —en adhesión al principio de minimización de datos y el viejo proverbio de seguridad de no poner todas las fichas en un mismo casillero. Sin embargo, aún no se tomaron decisiones y, con todas las idas y vueltas de los debates en varios WG, esto continuará siendo un acto de malabarismo.

Un tema candente en paralelo: el Nuevo IP

Con el descarrilamiento de la agenda, se canceló la mayoría de las reuniones paralelas que estaban planificadas. Aun así, algunas otras sí se llevaron a cabo, incluso sin haber sido bien publicitadas: sobre el debate del "nuevo IP", los escépticos podrían considerar que la falta de anuncios fue intencional.

Hace ya algún tiempo que se está tejiendo una disputa general sobre la iniciativa liderada por Huawei sobre un nuevo estándar de red post-IP. Miembros del Grupo Temático del UIT-T sobre Tecnologías de Red 2030 —un grupo formado en 2018 por el Grupo de Estudio 13 (SG13) del UIT-T— presentaron una propuesta de cara a la Asamblea Mundial de Normalización de las Telecomunicaciones (WTSA, programada del 17 al 20 de noviembre de 2020 en la India) para acelerar el trabajo del UIT-T sobre un protocolo de seguimiento para el TCP/IP. La motivación de este trabajo son las deficiencias que percibe el Grupo Temático con respecto a las aplicaciones de alta capacidad de las comunicaciones de vehículo a vehículo a las transmisiones holográficas.

¿Revuelo mediático contra China o sueños autoritarios?

Un extenso artículo en el Financial Times a finales de la semana del IETF provocó una mayor cobertura mediática y debate público sobre algunos aspectos de las características propuestas para el "Nuevo IP", lo cual no tiene nada que ver con el IP, según opinan algunos. Los aspectos más problemáticos que se han observado en varias presentaciones sobre el tema (por parte de investigadores y desarrolladores de Huawei y Futurewei) son la identificación electrónica (eID) aparentemente permanente que, opcionalmente, puede ser transmitida mediante cifrado, y la integración de funciones de un proveedor de red, gestor de ID y gestor de contabilidad en una red más integrada (con menos capas). El artículo del FT cita a Shoshana Zuboff, autora del *bestseller* "Surveillance Capitalism":

"Por supuesto que [China] quiere una infraestructura tecnológica que le conceda el control absoluto que han conseguido políticamente, un diseño que se ajuste al impulso totalitario", y agregó que esto "me da miedo y debería darles miedo a todas las personas".

Milton Mueller, de Georgia Tech, rechazó el artículo del FT por tener una línea argumental típica antichina y opinó que el Nuevo IP no era un debate nuevo, sino uno permanente y, en definitiva, era solo un proyecto de investigación. Richard Li, CTO de Futurewei, presidente del Grupo Temático de la UIT, presentó exactamente el mismo argumento. En un correo electrónico dirigido a la autora, Li enfatiza la naturaleza investigativa del Nuevo IP. Según Li, las consideraciones estuvieron impulsadas por una mayor demanda de capacidad y ancho de banda de las nuevas aplicaciones (contenido holográfico) y diferentes tipos de red (comunicaciones satelitales). Con respecto a las preocupaciones sobre las ID fijas y los comandos de desconexión, Li se refirió a trabajos previos del IETF como fuente de la división localizador-identificador (concerniente a eID) y al comando de desconexión (el WG de DOTS se menciona como una fuente). Los comandos de desconexión surgieron como resultado de los debates en DOTS (como la lucha contra DDoS).

Lo siguiente es un fragmento del correo electrónico de Li: *(...) eID y el Nuevo IP son dos temas distintos. Y el comando de "desconexión" ni siquiera forma parte del Nuevo IP. Los términos "eID" y "desconexión" aparecen por primera vez en las RFC del IETF y sus debates en grupos de trabajo. Hasta donde yo sé, el IETF ha estado estandarizando algunas características de identificador relacionadas con la seguridad, por ejemplo, en las implementaciones de Cisco y LISP del IETF. El comando de "desconexión" no es una característica del Nuevo IP bajo ningún punto de vista, sino que aparece por primera vez en DDoS Open Threat Signalling (DOTS) del IETF cuando DOTS intentó resolver el problema de DDoS para proteger a la red contra ataques de DDoS.*

Además, Li también remarca que el Nuevo IP no estaba completamente listo y que, sin lugar a dudas, sería interoperable con el TCP IP.

Aun así, se deben explorar varios aspectos. De hecho, la propuesta para la WTSA (TSAG-C133) no habla de investigación exclusivamente, sino que sugiere que los grupos de estudio del UIT-T relacionados (SG13, SG17, SG11 y SG20) deberían "preparar nuevas Preguntas (Q) para debatir las tecnologías orientadas a futuro que impulsan aún más la actual investigación". Se espera que los grupos de estudio produzcan estándares en el proceso habitual del UIT-T, de ser posible.

Otro indicador de que esta iniciativa se toma en serio podría ser el hecho de que el Grupo de Reguladores Europeos (que coordina el trabajo de preparación para la WTSA) incluyó en la agenda de su próxima sesión en mayo al Nuevo IP.

El ETSI crea su propio Grupo de Trabajo de Red No IP

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) anunció recientemente "la creación de un nuevo Grupo de Especificaciones de la Industria que abordará las Redes no IP (ISG NIN)". Según el comunicado de prensa, la reunión inaugural tuvo lugar el 25 de marzo, y John Grant, de BSI, fue electo presidente del ISG, mientras que Kevin Smith, de Vodafone, fue nombrado vicepresidente. Al igual que con el trabajo del Nuevo IP del UIT-T, la primera entrega es un informe sobre las deficiencias del IP (especialmente con respecto al 4G y al 5G, para los que el TCP/IP fue "considerado como no óptimo"). El nuevo grupo evolucionó a partir del Grupo sobre Protocolos de Próxima Generación del ETSI, creado en 2015. Los primeros "clientes" del ISG NIN podrían ser las redes móviles privadas, como la automatización de fábricas. En el comunicado de prensa, Smith expresó: "Sin lugar a dudas, la pila del IP y el modelo de capas OSI dieron paso a la conectividad global; sin embargo, al haberse originado en la década de 1970, su diseño es un reflejo de las demandas y las capacidades de esa era. La reevaluación de los principios fundamentales de diseño de los protocolos de red ofrece la oportunidad de incorporar beneficios de desempeño, seguridad y eficiencia para las redes de acceso y los casos de uso de 2020, y puede lograrse mediante la simplificación, en lugar de recurrir a complementos costosos. El trabajo del ISG NIN del ETSI, en cooperación con organizaciones de la industria,

puede brindar a los operadores una serie de protocolos de vanguardia que estos podrán agregar a su cartera de servicios".

Reacciones

El IETF criticó el esfuerzo respondiendo a una declaración de coordinación del UIT-T, advirtiendo que un "intento de diseño top-down en reemplazo de la pila de protocolo IP existente a gran escala sería dañino". Al reafirmar su liderazgo en la estandarización del IP en esa refutación, el IETF demuestra que no encuentra razón por la cual la serie de protocolos IP existente no pueda evolucionar para estar a la altura de los desafíos. La posición del IETF encontró apoyo en el trabajo de preparación para la WTSA del UIT-T; por ejemplo, por parte de RIPE NCC y la empresa British RTFM (conocida por muchos gracias a su fundador, Jim Reid).

Más HTTP: RIPT, WEBTRANS

El "encanto" de HTTP (Patrick McManus) está motivando a cada vez más WG a migrar aplicaciones al transporte HTTP. Como se informó previamente, un paso hacia el futuro HTTP podría ser un desarrollo para hacer que VoIP sea otra "aplicación HTTP".

WebTransport en lugar de WebSockets: ¿qué transporte usar?

Un enfoque diferente sería usar WebTransport. Está destinado a permitir que las aplicaciones restringidas se ubiquen en la parte superior del protocolo web y que, a la vez, no estén limitadas a flujos de datos individuales abiertos entre el cliente y el servidor como WebSockets, que se utiliza actualmente. WebTransport apunta a permitir flujos multiplexados una vez que se establece una conexión (flujo "conectado"). La opción también ayudaría a evitar el bloqueo de cabeza de línea. El WG de WebTrans, que se reunió por primera vez durante la reunión virtual, incluyó autores de Apple y Google y atrajo a muchos de los "sospechosos de siempre" de la comunidad de desarrolladores web en el IETF.

Uno de los temas principales sobre los que el WG debe tomar una decisión es qué transporte será la capa elegida para WebTransport, siendo las opciones HTTP2, HTTP3 y QUIC. Si bien muchos consideran necesario un potencial respaldo hacia TCP para permitir la compatibilidad con versiones anteriores, también surgió la idea de simplemente permitir, en cambio, la alternativa de volver a WebSockets.

Se debatió sobre la complejidad y el costo operativo de las diferentes variantes (HTTP2, HTTP3, QUIC), y se consideró como una posible manera de avanzar la necesidad de realizar pruebas prácticas de latencia en las diferentes variantes. Los resultados en cifras podrían ayudar a elegir un máximo de dos entre cuatro opciones de transporte diferentes. Tras la reunión, el WG dio inicio a la última llamada del documento de requisitos del WG.

Se tuvieron en cuenta posibles superposiciones con el trabajo de RIPT y MASQUE. Este último aborda el problema de que, al mudar el tráfico a QUIC/HTTP3, es necesario pasar del modelo de proxy (usado, por ejemplo, cuando se utiliza un proveedor de VPN) al mecanismo de multiplexación de aplicación en la parte superior de HTTP3. Luego de la autenticación mediante *handshake*, varias conexiones se pueden establecer dentro de la conexión QUIC, y se podrían utilizar varios proxies dentro de esta, en función de la respectiva demanda de la aplicación.

WG de DRIP: por primera vez, los legisladores van más rápido que los desarrolladores

La registración y la identificación en vivo de vehículos aéreos no tripulados (UAV o "drones") se han convertido en la prioridad número uno de los reguladores a ambos lados del Atlántico. Con la EASA y la FAA ponderando nuevas normas de registración, el WG del Protocolo de ID Remota de Drone (DRIP) quiere finalizar el *draft* de arquitectura y requisitos para julio: un plazo un tanto ambicioso.

Este grupo de trabajo es la creación de una sociedad entre AX Enterprise, una empresa consultora de software ubicada en Nueva York (con la reciente adjudicación de un contrato de USD 7,7 millones de parte del Laboratorio de Investigación de la Fuerza Aérea para estudiar cómo incorporar de manera segura a los drones en el Sistema Nacional de Espacio Aéreo militar y civil) y Robert Moskowitz, participante y consultor del IETF de larga data. Juntos, elaboraron un *draft* de requisitos y uno de arquitectura.

El objetivo es llenar los vacíos del estándar F3411-19 de la Sociedad Americana para Pruebas y Materiales (ASTM), un organismo de normalización radicado en EE. UU. que ahora es internacional. Hasta ahora, la ASTM se ha centrado en la recuperación a través de señales de radio de los datos de pilotos/propietarios de drones mediante Bluetooth, pero dado que el regulador estadounidense también hizo obligatoria una versión de red de acceso a datos, el IETF es un nuevo socio natural.

La propuesta actual apunta a HIPv2 y sus extensiones DNS. Con algunas adiciones menores a los protocolos del IETF (nuevos algoritmos de cifrado para HIP), la ID remota podría ser compatible tanto para el modelo de red como para el de señales de radio, según los autores. Los estándares existentes, como RDAP o EPP del espacio del DNS, podrían reutilizarse para la registración de datos y la consulta en vivo de propietarios/pilotos de drones a través de Internet.

La ventaja del acceso en capas a los datos sobre un drone y su propietario/piloto es la prevención de la filtración de datos privados, por ejemplo, en relación con los pilotos de drones o los modelos de negocios de drones comerciales (Walmart y Amazon podrían, en teoría, espiar mutuamente sus estrategias de entrega y sus bases de clientes). Con el modelo de privacidad propuesto, solo la policía y los

bomberos u otros solicitantes legítimos podrían ser capaces de acceder a la información sobre los drones y sus pilotos.

El enfoque actual de la EASA (artículo 14 del *draft* que implementa la regulación) obliga a todos los propietarios/pilotos de drones a tener registros de nombres claros de una manera que entra en conflicto con el GDPR, según los autores estadounidenses. Esperan que el acceso a una solución de protección de datos por diseño para la identificación y autorización de UAV ayude a los reguladores europeos a cambiar de opinión.

Vistazos de las reuniones de informes

Elegibilidad del Comité de Nominaciones en tiempos de coronavirus

La reunión virtual del IETF contó con dos reuniones de informes. La reunión de informes general abordó un problema relacionado con la crisis causada por el coronavirus: la elegibilidad del Comité de Nominaciones. Bajo las normas actuales, los candidatos para el Comité de Nominaciones del IETF deben haber estado presentes en 3 de las 5 reuniones más recientes del IETF. Estas normas se flexibilizarán mediante un documento especial (editado por el expresidente de la IAB, Brian Carpenter). Un intenso debate sobre este tema comenzó incluso antes de la reunión virtual del IETF, en una lista de correo electrónico especial.

Indicadores de compromiso

La copresidenta de las reuniones paralelas en curso de SMART, Kirsty Paine (National Cyber Security Centre/GCHQ), presentó un *draft* sobre los Indicadores de Compromiso (IoC) en lo que ella llamó un esfuerzo por compartir información entre la comunidad antimalware/LEA y la comunidad IETF para motivar a los operadores a permitir la visibilidad/gestionabilidad de estos IoC en sus redes y aplicaciones (ya sea mediante seguridad de endpoints o defensa basada en la red).

Algunos posibles indicadores de defensa enumerados en el *draft* son: direcciones IP, nombres de dominio, valores de Indicador del Nombre del Servidor de TLS, información de certificados, firmas como cadenas y patrones de código binario, hashes de binarios o scripts maliciosos, herramientas de ataque, como mimikatz [Mimikatz], y técnicas de ataque, como los boletos dorados de Kerberos [GoldenTicket].

El *draft* también afirma que tal información de IoC debería compartirse mediante plataformas especiales para la ciberdefensa.

Las reacciones ante el *draft* fueron variadas. Si bien varios participantes dijeron que el trabajo era interesante, muchos recomendaron que fuera una presentación independiente en lugar de un documento revisado por el IESG. De

todos modos, podrían llevarse a cabo debates de seguimiento en el WG de MILE en la lista de correo electrónico de OPSEC o en SAAG.

El RG de SMART, comenzado por el NCSC, junto con la exdirectora del Área de Seguridad, Kathleen Moriarty, hace varios años que intenta, sin éxito, crear un grupo en el IRTF. El grupo mantuvo reuniones paralelas durante las últimas reuniones del IETF y consiguió la presencia del CTO de NCSC en una de las reuniones de mayor convocatoria. Evidentemente, el presidente del IRTF no ha dado el visto bueno para establecer un grupo formal en el IRTF.

Una nueva IAB y otros vistazos de la Plenaria Administrativa

Durante la sesión plenaria virtual, la presidenta entrante de la IAB, Mirja Kuehlewind (Ericsson), recibió varias preguntas sobre transparencia. Particularmente, atrajo atención el acceso a los programas de la IAB que comienzan y, aunque varios de sus miembros, incluida Kuehlewind, acogieron con satisfacción ideas para nuevos programas de la IAB, incluso con expertos externos, la IAB también está debatiendo cómo organizará los programas en el futuro.

Kuehlewind hizo referencia a otro desafío que está enfrentando al comienzo de su mandato, con casi un 50% de miembros de la IAB que son nuevos en la junta, y el hecho de que las reuniones presenciales no son actualmente una opción a causa de la crisis por COVID-19.

El recambio parece, en parte, ser el resultado de que la editora de las RFC haya dejado el cargo. Algunos miembros de la comunidad piensan que esto fue una consecuencia de una mala administración por parte de la IAB, y se especula que podría haber sido la razón por la cual Ted Hardie no se presentó como candidato para un segundo mandato.

Junto con Hardie (Google), también dejarán la IAB Martin Thomson (Mozilla), Eric Nordmark (Zededa), Brian Trammell (Google), Christian Huitema (independiente), y Melinda Shore (Fastly). A Kuehlewind la acompañarán Ben Campbell (independiente), Cullen Jennings (Cisco), Jared Mauch (Akamai), Tommy Pauly (Apple), y Jiankang Yao (CNNIC).

Noticias de los nuevos participantes del IETF indican que, por primera vez, un empleado de Facebook (Murray Kucherawy) se unirá al IESG como director del área de ART. Cabe señalar que, si bien hay una buena representación del sector móvil y del sector web, no hay mucha participación de personas con experiencia en el funcionamiento del DNS clásico. (Para conocer todas las caras nuevas, consulte las diapositivas de la plenaria).

Está previsto que la reunión IETF 108 se lleve a cabo de forma online del 27 al 31 de julio de 2020.