INFORME IETF 92

Dallas

22-27 marzo 2015

Monika Ermert
para

CENTR &
LACTLD

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

LACTLD agradece la colaboración de CENTR por los aportes fundamentales para el financiamiento de la iniciativa, así como al apoyo de ISOC y la contribución de Hugo Salgado. Para acceder a la versión en inglés de este informe: https://centr.org/CENTR-Report-IETF92

LACTLD
Latin American and Caribbean ccTLDs Organization

https://centr.org/CENTR-Report-IETF92

Contenido

Destacados

El trabajo sobre la privacidad en el DNS, tanto en Operaciones del Sistema de Nombres de Dominio (DNSOP por sus siglas en inglés), como en DPRIVE se ha convertido en un tema central en muchas áreas (para el área de Transporte, véase más abajo), de las cuales el viejo y querido DNS es solo una.

En cuanto a la elección de propuestas, parece que, por el momento, DNS sobre TLS prevalecerá en el GT sobre DPRIVE, pero aún falta mucho para la implementación. Si bien algunos operadores señalan la necesidad de mantener el control sobre el tráfico del DNS por razones de monitoreo de seguridad, la decisión también está influida por la manera en la que cada solución afecta el modelo de negocios respectivo. Por ejemplo, la minimización de los datos los mantiene fuera del alcance de los operadores de la zona raíz.

Trabajo sobre la privacidad en el DNS: DNS sobre TLS recibe el visto bueno

DNS sobre TLS parece ser la variante preferida para las consultas y respuestas más privadas. Después de una ronda no concluyente de votos sobre el posible agrupamiento de distintas soluciones, el GT sobre DPRIVE expresó una clara preferencia por esta opción (y, a la vez, por DNS sobre TCP). Entretanto, este "consenso aproximado" fue confirmado en la lista de DNSOP. DNS sobre TLS es el documento conceptual preliminar propuesto por los investigadores de VeriSign Lab, de VeriSign Inc. (además de Paul Hofmann, quien presentó el documento preliminar).

De los tres documentos preliminares que proponen un DNS más privado presentados y que fueron considerados en Dallas, "Private DNS" (DNS privado) (de Philip Hallam-Baker, de Commodo) fue el que obtuvo menos apoyo, mientras que "Confidential DNS" (DNS confidencial) (de Wouter

Wijngaards, de Nlnet Labs y Glen Wiley, de VeriSign Inc) salió segundo, según los votos de los participantes en el GT sobre DPRIVE.

"Confidential DNS"

Wiley presentó los cambios realizados a "Confidential DNS" como una simplificación en relación con versiones anteriores. El concepto central del documento preliminar sigue siendo el nuevo registro de recursos (RR) "ENCRYPT", estructurado como flags, algoritmo, ID (en decimales), y datos (en base-64). Para intercambios salto a salto, el nombre de dominio del registro ENCRYPT es '.' (la etiqueta de la raíz). El cliente recoge el RR ENCRYPT del servidor que quiere contactar. La clave pública obtenida como resultado del RR ENCRYPT es utilizada para encriptar un secreto compartido o una clave pública que el cliente utiliza para encriptar las secciones de consulta de DNS y que el servidor de nombres de dominio, a su vez, utiliza para encriptar la respuesta. La clave es refrescada una vez pasado el TTL. Si falla la obtención de la clave o la consulta encriptada, se recurre al DNS sin confidencialidad.

El DNS confidencial ofrece tanto una versión oportunista como una autenticada, en este segundo caso, utilizando DNSSEC. Para el servidor de autoridad, la versión autenticada tiene la clave incluida en un registro de DS extra en la delegación del padre. Para los servidores recursivos, la clave está en la dirección IP invertida.

El principal defecto de "Confidential DNS" es que, a diferencia de DNS sobre TLS, su implementación todavía no se ha realizado: ha sido implementado "solo en sueños", dijo Wiley.

DNS sobre TLS

El DNS sobre TLS también sufrió algunos cambios en su nueva versión. En particular, ahora incluye un mecanismo en dos etapas. Primero, un cliente intentará iniciar una conexión TLS sobre un puerto especial recién asignado. Si el puerto está disponible, se abre la conexión. Si está bloqueado, debe establecerse la conexión enviando una consulta real o simulada sobre el puerto 53. El pedido debe ser marcado con un flag EDNSO "TLS Ok" (TO). Si al cliente le llega el bit TO de vuelta, se puede establecer la conexión DNS protegida por TLS. La orden de utilizar el cifrado basado en puertos o iniciar el cifrado basado en TLS puede darse localmente.

Si TLS falla, se recurre al DNS plano. Según Paul Hoffman, que se incorporó al grupo redactor de DNS sobre TLS (y anunció que se retirarían tres propuestas alternativas), el grupo decidió no hacer que la gente tuviera que pensar cómo cambiar el DNS. En cambio, los clientes deben saber cómo hacerlo. El bloqueo a través de los dispositivos intermedios puede crear problemas para DNS-sobre-TLS (véase la RFC 3207). El documento preliminar describe las siguientes situaciones:

a) El cliente del DNS envía T0=1 y recibe T0=0 → recurrir a la encriptación normal
b) El cliente del DNS envía T0=1 y recibe T0=1: el dispositivo intermedio no entiende la negociación de TLS→ si se aclara, seguir adelante, si no, recurrir a la encriptación normal o volver a intentar
c) El cliente del DNS envía T0=1 y no recibe respuesta → recurrir a la encriptación normal, reintentar más tarde

En general, los clientes que intentan usar TLS y fracasan pueden recurrir al DNS sin encriptación, o

esperar y volver a intentar más tarde, dependiendo de sus requisitos de privacidad.

Una cuestión que se planteó acerca de DNS sobre TLS fue qué hacer cuando hay múltiples aplicaciones que quieren abrir conexiones TCP/TLS (protocolo de control de transmisión/seguridad en la capa de transporte) al mismo tiempo. El número de consultas TCP puede ser mayor que el calculado, según Peter Koch (DENIC). Por ello, la sincronización inicial todavía requiere un debate. Paul Wouters (Apache) declaró que el uso de DNS sobre TLS no aporta un valor agregado cuando se está usando la encriptación de conexiones a través de una VPN (red privada virtual). Además, la gente no estaría a salvo de los resolvedores cuando utiliza esta opción, a menos que decidiera usar su propio resolvedor.

La opción DNS-sobre-TLS está dirigida principalmente a la gente que utiliza el DNS público sin una VPN: se trata de ofrecer "privacidad para todos" y "una forma de privacidad de alcance limitado", les dijo John Heidemann a los escépticos. Lo que hace que sea atractiva, según un representante de Microsoft, es que es el mecanismo que necesita "menos innovación".

Otra propuesta más: No se centren solo en TCP

Entretanto, se agregó otra solución posible, basada en el uso de DTLS/UDP en lugar de TLS/TCP. Los autores, Dan Wing y un grupo de Cisco, argumentan en contra de enfocarse en el uso de DNS sobre TCP debido al "bloqueo de encabezado de línea" y a la necesidad de completar las negociaciones en TCP para retomar las sesiones (más viajes de ida y vuelta). Hasta ahora, no ha habido suficiente apoyo para adoptar el documento preliminar sobre DTLS como documento del grupo de trabajo. Sin embargo, éste debate continúa.

Mediciones: Cuán privados son los mecanismos de privacidad del DNS

Esta vez, los investigadores de VeriSign Labs sí presentaron un documento preliminar sobre la evaluación de los mecanismos de privacidad. Según Allisen Mankin y sus co-autores, es necesario diferenciar mucho más qué nivel de privacidad brindarían los mecanismos propuestos de aumento de la privacidad del DNS. El grupo produjo un documento preliminar sobre "Evaluación de la privacidad para el intercambio privado en el DNS".

El aumento de la privacidad debería verificarse para las distintas conexiones:

Stub -> Recursivo
Stub -> Proxy
Proxy -> Recursivo
Recursivo -> Autoritativo

DPRIVE está estudiando principalmente la conexión Stub-Recursivo, pero la evaluación que busca mayor privacidad concierne a un espectro más amplio.

Otro aspecto para diferenciar/clasificar soluciones se vincula con la naturaleza del atacante. El documento preliminar enumera los siguientes: monitoreo generalizado (Tipo 1A), monitoreo directo (Tipo 1B, blanco específico) y monitoreo malicioso (Tipo 2). Los mecanismos listados incluyen redes de mezcla de tipo TOR, esconder las consultas en tráfico de relleno, técnicas de recuperación de la información privada, y cifrado. Los protocolos utilizados para estos mecanismos son, entre otros,

IPSEC, TLS (DNS sobre TLS) o TLS confidencial especial (que se describe en el texto como cifrado para propósitos especiales o DNS privado: cifrado para propósitos especiales con un agente de privacidad).

Los distintos conceptos poseen diferentes cualidades, y el mejor efecto posible se obtiene de una mezcla de varios mecanismos:

"Consideren un sistema hipotético en el cual puede implementarse tanto redes de mezcla (para lograr la no-relacionabilidad) como cifrado aleatorio (para evitar la detección), asegurando, así, la imposibilidad de observación, una cualidad más fuerte que cualquiera de las otras dos por separado".

Si bien, hasta cierto punto, es de poco interés práctico, clasificar los distintos mecanismos de esta manera podría ayudar a aclarar los posibles efectos y el esfuerzo necesario. El documento aún está siendo estudiado por el GT sobre DPRIVE.

Más trabajo sobre la privacidad en el grupo DNSOP

El GT sobre DNSOP también se refirió brevemente a otra propuesta de aumentar la privacidad: la minimización del qname. Uno de los autores del documento, Stephane Bortzmeyer, aludió a preguntas acerca de los posibles efectos negativos de la minimización de datos. VeriSign, en particular, ha llamado a considerar los posibles "efectos secundarios" desencadenados por la minimización del qname: "Si bien se aumenta la privacidad, también puede reducirse la visibilidad de las amenazas a la seguridad". Las colisiones de nombres, o una vulnerabilidad de ejecución remota de código anunciada recientemente por Microsoft, no se habrían detectado si se ocultaran las consultas completas de nombres de dominio a los servidores raíz. VeriSign urgió a que se analizara el tema en mayor profundidad y que se considerase la posibilidad de desarrollar "nuevos métodos para compartir información dentro del DNS" y, a la vez, enfatizó entusiastamente que está totalmente a favor de la minimización del qname. (VeriSign prometió una opción de licencia RAND para sus patentes vinculadas con qname. Habrá que ver en qué medida esta oferta atrae o disuade a los operadores.)

Otras preguntas que surgieron tienen que ver con el ocultamiento del qtype y con dos versiones alternativas de la minimización del qname: "agresiva" y "perezosa", y su oferta de distinta cantidad de datos. Si bien varias intervenciones destacaron que la privacidad era la motivación real, el GT no mostró ninguna preocupación por la pérdida de datos. Bortzmeyer afirmó que estaba claro que había actores con intereses diferentes e, incluso, en conflicto.

DNSOP está candente. Qué hacer con las solicitudes de nombres especiales

Una de las cuestiones más importantes que finalmente está abordando este GT es el tema de los nombres alternativos y la posibilidad de un segundo canal de solicitudes, además del de ICANN. La lista de solicitudes de nombres especiales (RFC 6761) empezó a crecer considerablemente en el último tiempo. Durante la sesión sobre DNSOP, se habló brevemente sobre dos de dichas solicitudes:

> Warren Kumari (Google) y Andrew Sullivan (Dyn) presentaron una propuesta de creación de .alt, un espacio alternativo para nombres que no se basan en la raíz del DNS, donde "no se aplican las normas habituales de registro ni de búsqueda". Ante la pregunta de si había interés en la creación de un espacio como ese, Kumari dijo que sí.

Se habló de .onion como etiqueta utilizada por la red TOR, que ya tiene otorgados alrededor de 30.000 nombres ".onion" (los nombres ".onion" marcan los servicios ocultos de TOR y son resueltos a través de los servidores de TOR, hashofpublickey.onion). TOR está intentando insistentemente ser aceptado como un TLD de uso especial debido a una decisión tomada por CA/Browserforum de dejar de otorgar certificados. Si .onion no recibe la aprobación del Grupo Directivo de Ingeniería de Internet (IESG por sus siglas en inglés), que está a cargo de las decisiones acerca de los TLD de uso especial, los certificados necesarios para las conexiones https://www.facebookcorewwwi.onion/, https://blockchainbdgppzk.onion/ o Intercept (https://y6xjgkgwj47us5ca.onion/) fallarán. Richard Baines (Mozilla), quien presentó el caso .onion, señaló razones más generales (y que también afectan a otros TLDs de uso especial) además del plazo de vencimiento de los certificados, como el constante filtrado de información posiblemente privada en el DNS, y el creciente número de consultas "bogus" en los resolvedores.

Otro grupo de solicitantes de TLDs especiales surgió del estudio sobre colisiones de nombres encargado por ICANN, pero, entretanto, los que presentaron la propuesta redujeron sus solicitudes de más de 6 a solo 2: home y corp. No obstante, este no es el final de la lista. También hay un pedido de un TLD experimental, no DNS, para el sistema de nombres GNU: .gns. En resumidas cuentas, los directores del GT mencionaron 41 solicitudes, lo que generó la preocupación de que el IETF pudiera atraer solicitudes que, por alguna razón, quieren eludir el procedimiento más tedioso (y caro) de solicitar los TLD a través de ICANN.

Los directores del GT quisieron postergar la mayor parte de la discusión para una reunión especial entre periodos de sesiones, planeada para el 12 de mayo, con una opción cara a cara para miembros del DNSOP que estén presentes en la reunión de RIPE en Amsterdam.

Innovar en Transporte. El grupo informal de discusión (BoF por sus siglas en inglés) sobre SPUD y el GT sobre "Seguridad aumentada en el TCP" o TCPINC

"Una serie de tubos": feroz debate sobre SPUD

Podría producirse un cambio fundamental en Internet si, además de convertirse en un Grupo de Trabajo del IETF, SPUD (las siglas en inglés de Protocolo Sustrato para Datagramas de Usuarios) fuera implementado ampliamente. Pero no vayamos tan rápido. SPUD es un producto del programa sobre evolución de las pilas de la IAB (Junta de Arquitectura de Internet), y de un taller realizado por esta en enero en Zurich sobre "la evolución de las pilas en una Internet de dispositivos intermedios" (SEMI por sus siglas en inglés). El debate fue altamente controvertido. Algunos lo ven como una "ofrenda de paz a los dispositivos intermedios", mientras que otros advierten que la neutralidad de la red podría verse afectada.

La idea básica es crear un mecanismo para agrupar paquetes UDP en un "tubo" con un comienzo y un final definidos en el tiempo. De este modo, sería más fácil mantener el estado. Los dispositivos entre los puntos finales que se comunican a través de SPUD pueden comunicarse explícitamente con los puntos finales fuera del contexto de la conversación punto a punto.

Los que presentaron SPUD dijeron que el motivo era liberarse de la inspección profunda de paquetes

pero, a la vez, posibilitar la administración de la red y transmitir la información necesaria para ello. Ted Hardie, de Google, explicó que podría ser necesario entregar alguna información a los dispositivos intermedios para obtener el transporte. Para diferenciar la UDP utilizada para SPUD del habitual uso basado en texto, se utilizará un bit mágico (primeros 32 bits).

Según Joe Hildebrand (Cisco), la Lista en los campos de encabezado de SPUD podría ser:

- un número mágico constante de 32 bits (d80000d8 (hex), o 1101 1000 0000 0000 1101 1000 (binario)
- 64 bits que definen la identificación de este tubo
- 2 bits de comando
- 1 bit que marca este paquete como declaración de solicitud (adec por la abreviatura en inglés)
- 1 bit que marca este paquete como declaración de ruta (pdec por la abreviatura en inglés)
- 4 bits reservados que DEBEN ser puestos a cero para esta versión del protocolo
- Si hay más bits, estos contienen un mapa CBOR

Durante la sesión BoF sobre SPUD, que contó con una nutrida asistencia, se plantearon varias razones por las cuales el IETF debería ocuparse de esta tarea:

- un intento de innovar el transporte (en las cada vez más “osificadas” capas de pila y transporte)
- permitir la administración de la red y, a la vez, proteger la privacidad haciendo que la inspección detallada de paquetes, que interrumpe el cifrado de punta a punta, sea innecesaria
- posibilitar la reducción de complejidad en la red de comunicación en tiempo real (RTC Web por sus siglas en inglés); SPUD debería ayudar a disminuir la complejidad ejemplificada por diseños como "encapsulamiento de SCTP sobre DTLS sobre ICE/UDP[, que] brinda una solución transversal para la traducción de direcciones de red (NAT por sus siglas en inglés)"

Si bien el nuevo concepto resuelve algunos temas vinculados con la Internet de dispositivos intermedios, también crea nuevos problemas. Uno es que, repentinamente, se inyecta en la red una nueva capa de meta información sobre paquetes de datos. Ted Hardie declaró que era necesario asegurarse de que la gente no cambiara su nombre a "Sr. Cabeza de papa". Debido a que la meta información podría filtrar repentinamente la información que la gente está tratando de proteger/ocultar en flujos encriptados, Mark Nottingham, de Akamai, advirtió que no se hicieran este tipo de cambios sin organizar un debate amplio (externo al IETF) ni brindar transparencia acerca de la meta información recién creada.

Aun cuando se está considerando el cifrado de la comunicación en esa meta capa, como observó Christian Huitema, de Microsoft (utilizando DTLS), el prototipo, que está siendo promovido actualmente para uso experimental, ha sido desprovisto de sus mecanismos de privacidad para facilitar el proceso. Finalmente, como Christian Huitema reconoció, SPUD también es propenso a nuevos ataques específicos. Por ejemplo, es bien posible que los atacantes envíen paquetes SPUD de cierre a los dispositivos intermedios, interrumpiendo los flujos de medios abiertos.

No se formó un GT, pero es muy probable que se continúe trabajando sobre el tema. Uno de los directores del BoF le dijo a esta periodista que es posible que se redacte un acta constitutiva preliminar, que se presentaría en otro BoF más adelante. Algunos de los asistentes desaconsejaron el abandono del principio punto a punto debido a la incorporación de una nueva meta capa. Un tema que vale la pena debatir es cuánto del esfuerzo de implementación de SPUD equivale a ofrecer un tratado de paz a los dispositivos intermedios (como lo describió Huitema) y cuánto, por el contrario, equivale a rendirse a

la Internet de los dispositivos intermedios. En lugar de hacer que el tráfico le hable a esos dispositivos, también podrían callarse y encriptarlo todo, observó un participante.

TCPINC

La encriptación del transporte además de la encriptación a través de la pila, como promueve el IETF en una declaración reciente, está, de hecho, sobre el tapete. El GT sobre TLS fue testigo de un feroz debate sobre la elección de TCPINC o TLS. No solo el DNS está buscando mayor protección contra el espionaje pasivo; el GT sobre TCPINC está haciendo lo mismo para el TCP, el protocolo de transporte. Los directores del GT y, más aún, algunos directores de Área, querían llegar a una decisión final sobre cuál de las dos opciones debería seleccionarse para seguir desarrollándola.

El protocolo que generó algún interés en los últimos meses es TCPCrypt, propuesto por un grupo de investigadores de Stanford (y otros). Según el documento preliminar, este protocolo podría brindar "cifrado no autenticado y protección de la integridad en la capa TCP". La idea es que las aplicaciones no tendrían que modificarse. Cuando los servidores acepten ejecutar TCPcrypt, se intercambiarán claves de cifrado utilizando la porción de datos de los segmentos TCP. Luego de ello, la encriptación aseguraría la confidencialidad y la integridad de las solicitudes transmitidas. Los ataques de degradación siguen siendo una posibilidad, así como los intermediarios, en los que un atacante controla parte de la red.

La segunda propuesta es reutilizar TLS para TCP: se negocia TLS al comienzo de una sesión TCP. La idea, según Eric Rescorla (Mozilla) – autor y gurú de TLS – es simple y, asimismo, está orientada a posibilitar que no haya que modificar las aplicaciones:

"Los mensajes SYN y SYN/ACK contienen opciones TCP que indican la voluntad de usar TLS y algo de información básica sobre las modalidades de TLS esperadas. Si ambos lados quieren usar TLS y tienen modalidades compatibles, los datos de la aplicación son protegidos automáticamente por TLS antes de ser enviados sobre TCP. Si no, los datos de la aplicación son enviados de la manera habitual".

Los participantes del GT no tomaron una decisión clara acerca de cuál elegir. Si bien algunos recomendaron dejar que ambos proponentes desarrollaran sus documentos preliminares (y trabajaran, por ejemplo, en poner a prueba su propuesta; Steve Kent, BBN), hubo un enérgico llamado a tomar una decisión e iniciar rápidamente la implementación de una opción (por ejemplo, por parte de Ted Hardie, de Google). Entretanto, el grupo académico empezó a implementar TLV y respondió a solicitudes de utilizarlo como protocolo de enmarcado. Aquí puede encontrarse un buen resumen. Ambas propuestas pueden ser obtenidas e implementadas en Github https://github.com/ekr/tcpinc-tls (TLS) y https://github.com/scslab/tcpcrypt (TCPCrypt). Implementar esta última puede hacerte entrar al "Salón de la fama de TCPCRYPT" ;-).

Privacidad del correo electrónico y una reapertura de OpenPGP en marcha

Desde la declaración del IAB en Hawai que se afirma que el aumento de la confidencialidad en la pila es prioritaria para el IETF. También existe una serie de mecanismos para aumentar aún más la privacidad de los correos electrónicos, por ejemplo, mediante la minimización de los meta datos.

Minimización de los meta datos: un agujero en la memoria

Dicha minimización ya podría realizarse fácilmente, según una propuesta presentada por Daniel Kahn-Gillmore, representante de la American Civil Liberty Union (Unión de derechos civiles de los EE UU), que se convirtió en asistente permanente en representación de las organizaciones de derechos civiles de EE UU. La idea se basa en la RFC 822 de la "edad de piedra", tal como fue utilizada en la RFC 6533. En el caso de correos que rebotan o que son reenviados, el encabezado ya no contendría el asunto. En cambio, este estaría integrado al cuerpo del mensaje. Un asunto que no es elegido con cuidado puede, a veces, revelar el mensaje principal (incluso si el cuerpo del mensaje está encriptado, por ejemplo, "Negociaciones del contrato: funcionaron"). Al poner el encabezado dentro del cuerpo del mensaje, que está encriptado, y un "asunto simulado" en el encabezado abierto, podría filtrarse menos información.

Según Gillmore, el mecanismo podría expandirse a otros campos de encabezado. Este concepto está siendo considerado en la comunidad de código abierto. Además, Gillmore mencionó que también se está analizando una solución para MIME. Es posible que se realice una introducción gradual para los Agentes de Usuario de correo electrónico (MUA por sus siglas en inglés). Para el próximo IETF, están en marcha los preparativos para reabrir el grupo de trabajo sobre OpenPGP a fin de realizar la tarea de mantención de este estándar o incluir otras tareas, por ejemplo, analizar el "agujero de memoria de los meta datos" de Kahn Gillmore.

Ladar Levison: Dark Mail

Ladar Levison (presunto proveedor de servicios de correo electrónico de Edward Snowden), quien cerró su empresa cuando fue citado por las autoridades estadounidenses para que entregara sus claves SSL para acceder al correo electrónico almacenado en versión cifrada en los servidores de Lavabit, presentó una idea creada fuera del IETF para aumentar la privacidad del correo electrónico en el grupo de trabajo de SAAG (Grupo Asesor sobre el Área de Seguridad). Levison, que se asoció con la empresa Silent Circle, de Phil Zimmerman, quiere crear un sistema de correo electrónico completamente nuevo para clientes preocupados por la seguridad/privacidad.

El conjunto de programas de Dark Mail incluye alternativas a IMAP (DMAP), SMTP (DMTP) y MIME (DIME), además de nuevos procesos de cifrado. Esencialmente, Dark Mail se basa en el cifrado de distintas partes del correo electrónico, una por una, como si fueran las capas de una cebolla y, finalmente, incluso oculta el remitente y el destinatario. Para usuarios no tan paranoicos, el correo sería enviado a un proveedor de correo electrónico, y el destinatario individual solo sería desencriptado allí. Además, los usuarios pueden incorporar material alternativo y más seguro para claves. Levison declaró que podría presentar estas propuestas para su estandarización por parte del IETF, pero que en este momento sigue intentando lanzar su proyecto y terminar el conjunto de programas.

Y más aumento de la privacidad...

Otro nuevo grupo de trabajo que se está ocupando de la privacidad es el "GT sobre Conferencias RTP (protocolo de transporte en tiempo real) de mayor privacidad" (PERC por sus siglas en inglés).

GTs y BoFs

DANE: El cambio de minúsculas a mayúsculas; la normalización sigue siendo un problema

Al haber muchos documentos que están avanzando por el proceso de RFC (DANE-SRV ya lo completó, DANE SMTP está en el IESG, "Actualización y orientación operativa para el Protocolo DANE y OPENPGPKey" llegó a la última llamada del GT), el Grupo de Trabajo se centró en el problema del cambio de minúsculas a mayúsculas y/o los pasos de la normalización para la parte local de las direcciones de correo electrónico.

Se considera que este tema, bien conocido, puede causar problemas para OPENPGPKEY (como también para MIME). Cuando se verifican claves (DNSSEC) con claves PGP en el DNS, puede producirse una discordancia debido a las distintas maneras de abordar el paso de minúsculas a mayúsculas de la parte local de la dirección. El acercamiento actual en el documento preliminar de Paul Wouters (Apache) es utilizar la solución elegida en la RFC 5321 y anteriores: que solo el MTA (agente de transporte de correo) receptor pueda interpretar la parte local de una dirección.

"Por ello, un cliente que opera con OPENPGPKEY NO DEBE ejecutar ninguna clase de reglas de mapeo sobre la base de la dirección electrónica. Como la parte local se convierte en minúsculas antes de realizar la función hash, las posibles diferencias entre mayúsculas y minúsculas no causarán problemas para la búsqueda de OPENPGPKEY". Aun cuando la discusión ha durado bastante tiempo en la lista de correos después del evento, la mayor parte de los expertos en correo electrónico piensan que no es un tema que pueda resolverse en el GT sobre DANE.

El GT presenció también una exposición de Eric Osterweil acerca del trabajo de VeriSign Labs sobre la actualización de la situación de la librería de S/MIME. Pueden examinarse las herramientas aquí:
https://github.com/verisign/smaug,
https://github.com/verisign/smaug-tbird-plugin

Osterweil también invitó a los presentes a que utilizaran el portal de suministro de DANE: https://dane-provisioning.verisignlabs.com/ (al que no pude entrar desde mi computadora).

Finalmente, el co-director del GT Olafur Gudmundson pidió a los participantes que consideraran la actualización de metas y la posibilidad de una renovación del acta constitutiva. Por ello, se trata de un buen momento para proponer nuevas tareas. Una cuestión que se planteó, el uso de DANE para la asociación de información sobre pagos, podría ser analizada por el GT. La propuesta redactada por VeriSign y Armory Technologies, proveedor del monedero Bitcoin, sostiene que "un registro de asociación de pagos asocia un identificador de servicios de Internet – por ejemplo, una dirección electrónica – con información sobre pagos: por ejemplo, un número de cuenta o una dirección de Bitcoin".

Según algunos expertos, con toda esta información adicional – información sobre claves y, potencialmente, sobre pagos – almacenada en el DNS, la necesidad de que los intercambios en el DNS sean más confidenciales (y más seguros a través de DNSSEC) se hace todavía más urgente.

Grupo de Trabajo sobre Extensiones al EPP (Protocolo de Aprovisionamiento Extensible): VeriSign registra el primer gran conjunto de extensiones

El grupo de trabajo sobre EPPext está cerca de completar sus temas de trabajo. En especial, estableció un proceso formal de registro para las nuevas extensiones EPP basado en la RFC 7451. Las primeras 18 extensiones EPP registradas con la IANA provienen de VeriSign. Se plantearon algunas inquietudes sobre las advertencias de derechos de autor que acompañaban las extensiones. ¿El nuevo proceso de registro cumplirá realmente su objetivo de administrar y coordinar mejor el desarrollo de extensiones EPP?

El IESG seleccionó una lista de expertos para revisar las extensiones presentadas por distintos registros/ distintas partes. Los evaluadores son: Scott Hollenbeck (VeriSign), principal, y Alex Mayrhofer (nic.at), Ning Kong (Cnnic), Roger Carney (GoDaddy) y Jim Galvin (Afilias), secundarios.

En concordancia con su acta constitutiva, el GT debatió acerca de una lista corta de extensiones que son candidatas para el nuevo registro: 1) Extensión para el Mapeo de Nombres de Dominio Internacionalizados para el EPP (de Uniregistry), que, según uno de los co-presidentes, Jim Galvin, necesita una sección de evaluación y una decisión acerca de si debería convertirse en norma o no; 2) Mapeo de extensiones para el relé de claves para el EPP (de SIDN), que, según Galvin, está lista para la última llamada, si es que no se decide que inicie el proceso de transformación en norma; 3) Fase de lanzamiento del mapeo del EPP (de VeriSign, Cloud Registry y Centralnic), que, según Galvin, también está lista para la última llamada. Se plantea nuevamente la pregunta de si se iniciará el proceso para que se convierta en norma y 4) Mapeo de Objetos de Marca y Marca Firmada (de ICANN), que, según Galvin, está lista para la última llamada e iniciará el proceso de transformación en norma.

El co-director del GT declaró que, desde el punto de vista procedimental, el GT busca diferenciar entre extensiones que se convertirán en RFCs, que pueden ser discutidas en el GT una vez que este haya reformado su acta constitutiva, y aquellos documentos que son solo informativos. Estos últimos solo serán revisados por los expertos designados y, teniendo en cuenta las solicitudes de que se cumpla con las obligaciones formales, serán enviados al registro de EPP de la IANA.

Aun cuando el GT no ha terminado de examinar la lista inicial de documentos ni de definir si estos deberían ser futuras normas o documentos informativos, y se siguen agregando nuevos documentos a través de la lista de correos, un primer gran grupo de 18 extensiones, todas etiquetadas como informativas, ya fueron presentadas por VeriSign, aprobadas y agregadas al nuevo registro de extensiones EPP de la IANA sin que el GT los analizara. El registro masivo realizado por VeriSign parece anticipar el futuro proceso para los documentos informativos. Luego de un breve intercambio sobre algunas cuestiones editoriales, además de una preocupación menor por la advertencia sobre derechos de autor que acompañó los documentos de VeriSign, Scott Hollenbeck los envió al registro de EPP. Alex Mayrhofer, de nic.at, escribió en su reseña que la advertencia de VeriSign sobre derechos de autor prohíbe la "copia o comunicación" del documento sin "previo consentimiento por escrito de VeriSign", lo cual, de hecho, dificultaría, incluso, ver el documento en la red.

Incluidas en el nuevo registro hay otras extensiones más antiguas que pasaron por el proceso de convertirse en normas: RFC 3915 (E.164 Mapeo de números para el EPP), RFC 5076 (Información de validación ENUM para el EPP) RFC 4114 (Mapeo del periodo de gracia para nombres de dominio para el EPP) y RFC 5910 (Mapeo de DNSSEC para el EPP).

Una cuestión interesante en relación con el registro del EPP es la pregunta de en qué medida este va a ayudar a "administrar y coordinar" el desarrollo de extensiones y, más específicamente, a evitar la duplicación de esfuerzos. Según la RFC 7451, "los expertos designados deberían ser permisivos en su evaluación de solicitudes de registro de extensiones que hayan sido implementadas y desplegadas por

al menos un par registro/registrador. Esto implica que se puede realmente registrar múltiples extensiones que brinden la misma funcionalidad. Las solicitudes de registro de extensiones que no han sido implementadas deberían ser evaluadas con el propósito de reducir la duplicación de funciones". A aquellos registrantes que quieran presentar una extensión que no ha sido desplegada, y que es similar en su funcionalidad a una ya registrada, se les pedirá que reconsideren su pedido.

Sigue abierta la pregunta de hasta qué punto las advertencias sobre derechos de autor, como las que acompañaron las extensiones registradas por VeriSign, se convertirán en una barrera para la armonización.

El paso siguiente para el GT, luego de completar su primer conjunto de documentos, es la posibilidad de reformar su acta constitutiva. Galvin señaló que este paso podría convertir al GT en el lugar oficial para las extensiones que quieren convertirse en norma (siempre que haya documentos en preparación). Otros temas de interés que mencionó fueron los desarrollos de Whois en relación con ICANN y los Talleres de Operación de Registros (ROW por sus siglas en inglés), que se han realizado dos veces en colaboración con el IETF y están en camino de convertirse en un evento institucionalizado que vincula el trabajo de normalización y el trabajo operativo. El próximo ROW tendrá lugar el 19 de julio en Praga, en paralelo al IETF 93.

BoF sobre MODERN: ¿retomar lo que ENUM interrumpió?

El IETF inicia nuevamente la discusión sobre numeración de voz a partir de propuestas de Henning Schulzrinne (Comisión Nacional de Comunicaciones de EE UU) y Jon Peterson (Neustar, que es, de hecho, proveedor del Registro Norteamericano de Números). ¿Le gustará a la UIT?

La idea básica es que MODERN "definirá un conjunto de mecanismos basados en Internet para administrar y resolver números telefónicos (NTs) en un entorno IP". Los proponentes sostienen que, considerando que la voz está siendo incorporada gradualmente a todos los IP, es necesario que un nuevo sistema administre los NTs, por las siguientes razones:

- el modelo según el cual los NT tienen una asociación con un único proveedor de servicios no existe más;
- el localizador de red desaparece (en cambio, el NT identifica a un individuo o a una organización);
- cada vez más, los dispositivos, las aplicaciones y las herramientas de la red tienen que solicitar y adquirir delegaciones de NTs de las autoridades.

Sería posible utilizar tanto un árbol jerárquico como un P2P para la administración de los números. Se dice que la privacidad de dicha administración es de sumo interés.

Si bien en Dallas hubo una considerable disposición a la creación de un GT, ahora se plantean preguntas sobre si el nuevo marco cambiaría el modelo de asignación de números: de un modelo de dos niveles, a la asignación directa sin necesidad de transferencias. ¿Acaso llevaría a una mayor centralización (con la eliminación de los registros nacionales de números)? Como lo demuestra la discusión en la lista que incluye representantes de los operadores, existe bastante resistencia a la "extralimitación" de un nuevo GT, y hubo quienes señalaron el fracaso de ENUM.

Jon Peterson, que presentó el planteamiento del problema al GT, explicó que las limitaciones del DNS (sintaxis rígida y aumento de la complejidad al agregar seguridad) motivaron la idea de desarrollar un "marco y modelo de información independientes para las consultas y respuestas vinculadas con números de teléfono y enrutamiento de llamadas que permitan una expresión más rica tanto de las preguntas como de las respuestas".

Lo que sigue son los temas de discusión enumerados en el acta constitutiva preliminar:

- una reseña de la arquitectura que incluya requisitos de alto nivel y consideraciones sobre la seguridad/privacidad;
- una descripción de los procesos de suscripción para NTs ya existentes y nuevos, incluyendo toda modificación de los meta datos vinculados con esos NT;
- una descripción de los mecanismos de protocolo para acceder a la información de contacto asociada con las suscripciones;
- una descripción de mecanismos para resolver información relacionada con los NT;
- un mecanismo de protocolo para resolver NTs que permita que entidades tales como proveedores de servicios, dispositivos y aplicaciones tengan acceso a datos relacionados con los NT, posiblemente incluyendo datos del nombre de la persona que llama (CNAM).

Debería considerarse el trabajo con ENUM, SPEERMINT y DRINKS. Es posible que se forme otro BoF que, a su vez, puede llegar a constituirse en GT.

La selección de nuevas curvas para TLS por parte del Foro sobre Investigación sobre Cifrado (CFRG por sus siglas en inglés): un proceso problemático

Después de un proceso bastante complicado, los co-directores del CFRG se decidieron por la Curva 25519 (Dan Bernstein) y la Goldilocks (Mike Hamburg, MIT). Habrá mucho que hacer cuando el IETF quiera crear su propio flujo de estándares sobre criptografía.

El CFRG eligió dos nuevas curvas para el cifrado en la Seguridad de la Capa de Transporte (TLS por sus siglas en inglés). Una es la curva 25519 (y^2 = x^3 modulo p = 2^255 – 19), elaborada por Dan Bernstein (Universidad de Chicago y de Eindhoven); la otra, mucho más reciente (x2 + y2 ≡ 1 - 39081x2y2 mod 2448 - 2224 – 1), fue diseñada por Mike Hamburg. Hamburg es un colega de Bernstein que colaboró con este.

Las curvas son similares, en el sentido de que ambas son elípticas y que los criptógrafos reconocen que son más rápidas y seguras para los ataques de canal lateral. Ambas han sido caracterizadas como seguras por el proyecto de curvas seguras. La diferencia más obvia es que la de Bernstein existe desde 2006 y no se le conoce ningún ataque exitoso, mientras que Goldilocks es nueva: fue creada en 2014. En segundo lugar, 25519 permite un nivel de seguridad de 128 bits, mientras que Goldilocks llega hasta un nivel de 223 bits. Según el presidente del GT sobre TLS del IETF, Paterson, este grupo había solicitado curvas de 128 bits y más. Ambas son más rápidas que las del NIST (Instituto Nacional de Normas y Tecnología de EE UU) que han estado en uso hasta ahora. Los participantes en el CFRG, especialmente Microsoft, habían pedido que se incluyera una más grande en la propuesta presentada al GT sobre TLS. Microsoft tenía la esperanza de que las curvas de su equipo fueran las elegidas, pero estas fracasaron luego de un feroz debate en la lista de correos.

El CFRG no logró consenso, por lo cual los directores del GT decidieron qué curvas elegir sobre la base de respuestas a una encuesta. A diferencia del IETF, en el IRTF los directores están habilitados

para tomar esa decisión. En la reunión del GT en Dallas, Paterson insinuó que habían surgido animosidades durante el debate, pero dijo que luego de que la decisión fue tomada por los tres presidentes, el clima en la lista de correos mejoró mucho.

Dos expertos en criptografía que hablaron con esta periodista señalaron lo que ellos consideran como deficiencias del proceso de selección. Uno argumentó que, tal como había sido concebido, este proceso implicaba decidir primero sobre un documento de requisitos, y recién entonces elegir entre las propuestas presentadas. El otro señaló que hubo intentos de presionar a los directores para que aceptaran o rechazaran ciertas curvas.

El hecho de que el IETF elija los estándares criptográficos para sus propios protocolos y conjuntos de protocolos es el resultado de revelaciones en los documentos hechos públicos por Edward Snowden, el denunciante estadounidense. Luego de que el NIST debió confirmar que la NSA (Administración Nacional de Seguridad de EE UU) había manipulado la selección de algoritmos en al menos una instancia (reduciendo el grado de arbitrariedad de los números arbitrarios), el IETF inició un proceso para elegir sus propios algoritmos o, mejor, para hacer que el CRFG evaluara y recomendara posibles candidatos.

Aun cuando la mayoría de los participantes pueden estar de acuerdo en que, hasta ahora, el proceso ha sido problemático, muchos piensan que los resultados son positivos. Paterson bromeó durante la sesión del GT, diciendo que podía asegurarle al grupo que el proceso no había sido manipulado, "al menos por mí". Un problema sistemático de la selección de estándares criptográficos es que la matemática involucrada es accesible solamente a los expertos. Incluso, muchos de los participantes en el GT dicen que no pueden evaluar las curvas.

Los funcionarios del NIST habían advertido al IETF que no tenía suficiente excelencia criptográfica entre sus miembros para elegir sus propias curvas: ¿un intento de desalentar al IETF/IRTF en sus esfuerzos por lograr la autonomía criptográfica?

El presidente del GT, Sean Turner, declaró que ahora que la selección había sido hecha, esperaba que su grupo (y otros) presentaran más solicitudes al CFRG para que proporcionara criptografía para los protocolos del IETF. La mayoría de los miembros del CFRG acordaron que sería bueno, pero no necesario, que el NIST reconociera el estándar del IETF. No obstante, el GT alentó a los directores a anunciar y presentar las curvas seleccionadas durante una próxima reunión organizada por el NIST que abordará la selección de nuevas curvas. El trabajo realizado por el CFRG para el GT sobre TLS estará completo cuando se elijan los estándares de firma. El CFRG presentará al GT el paquete completo de curvas y algoritmos de firma.

Novedades del IETF

La Fundación del IETF será titular de los derechos de autor (y los dominios) vinculados con la IANA
Andrew Sullivan (DYN), nuevo presidente de la IAB
El IETF viaja a Latinoamérica por primera vez en 2016

El traspaso de la IANA y sus derechos de autor

El entonces director de la Fundación del IETF (IAOC Trust), Tobias Gondrom, informó que la Fundación estaba dispuesta a convertirse en titular de los derechos de autor para la IANA. La respuesta

fue provocada por un pedido del ICG (el grupo que coordina el traspaso de la IANA). La reunión del GT sobre el Plan para la IANA – el espacio oficial para la presentación de la propuesta de traspaso por parte del IETF – que debía tener lugar en Dallas fue cancelada. El presidente del IETF, Jari Arkko, señaló durante la plenaria que la comunidad del Foro estaba esperando que la comunidad de ICANN finalizara su propuesta para la futura supervisión de los servicios vinculados con los nombres de dominio de la IANA.

Nuevo director de la IAB (Internet Architecture Board)

La IAB tiene un nuevo director, Andrew Sullivan, del área de DNS de DYN, que reemplaza a Russ Housley (Vigil Security). Housley fue director del IETF durante el máximo tiempo permitido (dos mandatos), y se lo mantuvo como líder una vez que su período como presidente llegó a su fin. También ejerció la presidencia de la IAB durante el máximo tiempo permitido (dos mandatos). Obviamente, el hecho de que fuera patrocinado explícitamente por la NSA no fue considerado como un problema por los miembros. Su reemplazo por Sullivan también implica el cambio de un experto en seguridad por un experto en el DNS. Sullivan fue co-director de DNSEXT cuando se estandarizó el DNSSEC y, además, participó en una serie de reuniones de ICANN y del IGF.

Reuniones y visas

Por primera vez en su historia, el IETF se reunirá en Latinoamérica en 2016. El encuentro en Buenos Aires será preparado mediante una serie de talleres en países latinoamericanos organizados por ISOC.

Tobias Gondrom, del IAOC, informó que el tan debatido problema de la visa para ingresar a los EE UU para la reunión de Dallas pudo resolverse más fácilmente que en años anteriores. En un esfuerzo por dar más tiempo para solucionar problemas de visa y preparar los viajes, la inscripción a las reuniones generales se iniciará con mayor antelación. La inscripción para Praga se abrió inmediatamente después del encuentro en Dallas.

La próxima reunión del IETF tendrá lugar en Praga del 19 al 24 de julio.