INFORME IETF 92

Praga

20-24 julio 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-IETF93

Contenido

Destacados 2
De punta a punta, menos metadatos, la próxima generación del DNS 2
Separar "identidad" de "persona" 3
Ajustarse a los principios 3
No nos peleemos, pide el Secretario General de la UIT 4
Nuevo round en la controversia sobre nombres especiales 5
División en la comunidad técnica debido a la reserva de nombres que no son del DNS a través del IETF 5
Deshacerse de la 6761: la ocupación ilegal de .local sentó un mal precedente 7
El proceso de reserva es poco claro 7
Criptografía cuántica: No la dejen para más adelante 8
DNS: "Privacidad bastante mala" 9
Los ataques de canal lateral sobre DNS y qué hacer para evitarlos 9
Problemas con el DNS encriptado 10
Grupos de Trabajo y BoFs 11
DANE: Incorporarlo a la infraestructura básica 12
QUIC: ¿mucho mejor que el TCP? 12
EPPEx 13
EPPExt 13
Novedades del IETF 13

Destacados

Dos invitados sorpresa sumamente diferentes: Edward Snowden y Houlin Zhao

El primer invitado sorpresa, Edward Snowden, se sumó a los participantes en la reunión del IETF para una hora de preguntas y respuestas luego de la proyección del documental *Citizen Four*. Snowden recomendó a la comunidad del IETF que la estandarización no se realizara según la conveniencia de los Gobiernos ni de las corporaciones. Antes bien, deberían "asegurarse de que los estándares, nuestra tecnología, los sistemas trabajan para proteger y defender las intenciones de los usuarios".

De punta a punta, menos metadatos, la próxima generación del DNS

Según Snowden, el camino a seguir para la estandarización es considerar el principio estándar de la seguridad de punta a punta. Este ha sido comprometido, y la "idea de un núcleo simple y bordes inteligentes se transformó en bordes muy tontos y un núcleo letal". Cuando señaló que todos los

dispositivos intermedios que interfieren la comunicación de punta a punta hacen que surjan posibles vulnerabilidades, el ex analista de la NSA (Administración Nacional de Seguridad de los Estados Unidos) recibió una salva de aplausos. Snowden también advirtió que la ruta de red "es actualmente la parte más peligrosa de la red". Los ingenieros deben "ayudar a los usuarios a atravesarla sin peligro".

Acerca de los metadatos, Snowden afirmó que no debería olvidárselos en el camino hacia la "encriptación masiva", la cual, en su opinión, será implementada en los próximos 15 a 20 años. Los organismos de inteligencia y las empresas todavía encontrarán todo tipo de razones para utilizar metadatos para monitorizar la actividad de los usuarios y trazar su perfil por asociación o ubicación. Citando al ex presidente de la NSA, Michael Hayden, Snowden señaló: "Matamos basándonos en metadatos", refiriéndose a los ataques con drones realizados por las fuerzas armadas estadounidenses. A pesar de que el plan original era que la tecnología de vigilancia fuera acotada, esta se comercializó fácilmente luego de que algunos empleados de la NSA dejaron el organismo para crear sus propias empresas y la lanzaron al mercado."Si se están creando más metadatos, eso es malo en términos generales", comentó en relación con los nuevos protocolos. También mencionó las ideas que se conversaron recientemente en el grupo de trabajo sobre SPUD como ejemplo de los efectos negativos de la creación de otra capa de fuentes de metadatos sobre las intenciones de los usuarios.

Snowden se refirió específicamente al DNS como otra fuente de metadatos. Si el contenido estuviera siempre encriptado pero las solicitudes del DNS no lo estuvieran, los usuarios aún podrían ser identificados mediante inferencias estadísticas. Por ello, Snowden elogió los esfuerzos de los grupos de trabajo sobre Dprive y DANE, y dijo que la implementación del DNSSEC, si bien no podría considerarse como el huevo de oro, sí es "mejor que lo que tenemos ahora". "Cuando se combinan [Dprive, DANE y DNSSEC], se crea la próxima generación de DNS". Al elaborar estos estándares, los ingenieros tuvieron que considerar la necesidad de "crear una Internet que sobreviviera no solo unos años, sino cien años o más".

Separar "identidad" de "persona"

Su principal recomendación vinculada con la privacidad fue la siguiente: "Tenemos que separar la identidad de la imagen pública de manera duradera". Snowden recomendó considerar sistemas alternativos de asignación de nombres. Contrariamente a lo que sucede con el pago de tarjetas de crédito, es necesario elaborar y aplicar conceptos para el pago anónimo, por ejemplo, el pago con vales. Snowden urgió a que los usuarios puedan elegir utilizar una "persona común, no persona o persona anónima" para transacciones en la red. Los identificadores de hardware globalmente únicos también constituyen un problema para la privacidad, afirmó, y, además, cuestionó el uso actual de direcciones MAC (por sus siglas en inglés; en español: control de acceso al medio).

Ajustarse a los principios

Además de criticar la vigilancia masiva, Snowden aplaudió los esfuerzos del IETF, y dijo que el proyecto de estandarización de Internet es hoy más abierto que nunca. Si la tecnología se convierte en un peligro, es porque la dejamos en manos de otros, afirmó durante el período de preguntas y respuestas.

Finalmente, planteó su preocupación acerca de los intermediarios, cuyas acciones se oponen a los intereses del proceso de estandarización de Internet y recuerdan las intervenciones de la NSA sobre el estándar Dual_EC_DRBG, proceso del cual el NIST (Instituto Nacional de Estándares y Tecnología de EE UU) se retiró. Afirmó que, durante su trabajo para la NSA y la CIA, había observado que se

enviaba gente a trabajar en grandes organizaciones: no en organismos de estandarización, pero sí en empresas de infraestructura. Se les decía a esas "mulas" que tenían que alejar a la organización de tal cosa y acercarlos a tal otra porque la segunda era más segura cuando, en realidad, esta última ofrecía una puerta trasera para la agencia. De hecho, las mulas estaban "haciendo cosas malas por buenas razones" y, en lugar de sospechar del "tipo de bigote", Snowden propuso centrarse en los principios mismos, entre ellos, proteger las intenciones de los usuarios. Si algo parece sospechoso, en lugar de tratar de analizar quién está detrás y con qué objeto, los ingenieros deberían examinar el elemento en cuestión y encontrar las debilidades para impedir que se adopte.

Snowden recibió un aplauso cerrado y, a lo largo de la reunión del IETF, muchas personas dijeron que sus presentaciones habían sido lo mejor de la semana, si bien no se trató de una actividad formal del IETF, como subrayó Mark Nottingham. Obviamente, se consideró que una invitación a la plenaria técnica oficial constituía una medida demasiado audaz. Nottingham había co-organizado el evento con Daniel Kahn Gillmor (de la ACLU, la organización de derechos civiles de los EE UU). Ahora también se está considerando invitar a Snowden a la próxima reunión del W3C.

No nos peleemos, pide el Secretario General de la UIT

El segundo invitado sorpresa al IETF fue el nuevo Secretario General de la Unión Internacional de Telecomunicaciones, Houlin Zhao. Esta fue la primera visita de Zhao al IETF luego de haber sido elegido por los Estados Miembros de la UIT el 23 de octubre para reemplazar a Hamadoun Touré. El foro e ISOC ya lo habían invitado para la reunión de Hawai en noviembre de 2014. Antes de su designación, el diplomático de carrera había trabajado en la UIT-T (el sector de normalización de la UIT) desde 1986. Luego fue Director de la Oficina de Estandarización de las Telecomunicaciones (1999-2006) y Subsecretario General de la UIT (2007-20149).

Zhao fue uno de los oradores de la plenaria de la Junta de Arquitectura de Internet. Su principal mensaje a la comunidad del IETF fue un llamado a la cooperación entre los distintos organismos de normalización, más allá de sus respectivos modelos de gobernanza (intergubernamental o de abajo arriba). Declaró que "algunos podrían considerar a la UIT como de arriba a bajo, pero ya sea de arriba abajo o de abajo arriba, servimos al mismo mercado". Las organizaciones deberían evitar pelear por sus respectivos campos, urgió el nuevo Secretario General, pero no se refirió en ningún momento a las disputas recientes, como la que se generó respecto de la "bifurcación" de MPLS por parte de la UIT.

Zhao recordó a los participantes la formación de la Organización de Apoyo a los Protocolos (PSO por sus siglas en inglés), y afirmó que quizá fuera hora de abrir una nueva página en la relación entre las organizaciones. La PSO, creada por la IAB, la UIT, W3C y el Instituto Europeo de Estandarización de las Telecomunicaciones (ETSI por sus siglas en inglés), rotaba directores a la Junta de ICANN, pero fue disuelta en noviembre de 2002. El organismo que la sucedió fue el Grupo Técnico de Enlace, y la banca de director en ICANN fue rebajada a una representación sin voto. Finalmente, un cambio de estatuto de 2013 creó un enlace con la Junta de ICANN exclusivamente para el IETF. La UIT, ETSI y W3C ya no tienen representación directa en la Junta.

La relación entre el IETF y ICANN se fortaleció durante la presidencia de Fadi Chehade.
En este contexto, la visita del Secretario General de la UIT, que fue recibida con un aplauso cortés (aunque algo frío) por los participantes en la reunión de la IAB, pareció un intento de recuperar terreno. No obstante, en vez de ofrecer propuestas concretas de "cooperación", Zhao realizó el gesto simbólico de ponerse la camiseta del IETF 46 sobre su camisa.

Nuevo round en la controversia sobre nombres especiales

La reserva de un nombre especial, .onion, para el proyecto TOR se encuentra en la última etapa, y se puede ofrecer comentarios hasta el 11 de agosto. Sin embargo, la batalla sobre cómo interpretar e implementar la RFC 6761 – "Nombres de dominio para usos especiales" – prosiguió con furia en la lista de correos, tanto antes como después de la reunión del Grupo de Trabajo sobre DNS OP. En la reunión del GT, los presidentes anunciaron que piensan establecer un equipo de diseño que estudie la 6761 para aclarar las dudas que el GT empezó a analizar cuando consideraba las solicitudes de nombres especiales. Para algunos, se trata de un intento de cerrar la puerta al registro de nombres alternativos antes de que el IETF se meta en problemas políticos con ICANN.

Durante la sesión del DNSOP, Christian Grothoff, de INRIA, presentó las solicitudes de TOR (además de .onion, .exit y, posiblemente, .tor) y un grupo de proyectos P2P, entre ellos, el Sistema de Nombres de Gnu (GNS por sus siglas en inglés) – .gnu – el Proyecto Namecoin – .bit – y el Proyecto I2P – .i2p – . Todos se basan en protocolos diferentes del DNS, pero utilizan cadenas de nombres como identificadores. Grothoff explicó que los proyectos P2P ya existían desde hace un tiempo, y querían utilizar el proceso de la 6761 para documentar el uso de nombres con la idea de intentar evitar colisiones con nombres del DNS que ICANN podría delegar en el futuro. "¿Sería mejor si no delegáramos?", fue su pregunta a la comunidad del IETF. Además, anunció que se esperaban otras solicitudes de nombres especiales por parte de la comunidad P2P.

División en la comunidad técnica debido a la reserva de nombres que no son del DNS a través del IETF

El GT sobre DNSOP, y el IETF en su totalidad, está claramente dividido en lo que se refiere al manejo de las solicitudes para nombres especiales según la RFC 6761. Esta RFC fue introducida por Steward Cheshire, de Apple, para la reserva de .local (RFC 6762). El autor de las dos RFCs defendió el proceso establecido en la 6761. Como en el caso de .local, hay nombres que no son de DNS, pero solo se resolverían localmente, una cuestión que también enfatizó Grothoff, quien dio como ejemplos *.ipv6.literal.net* y *pnrp.net*, de Microsoft. Cheshire planteó que, en lugar de hacer de cuenta que "somos la única alternativa, tenemos la función de administrar el espacio común de nombres ".

Stephane Bortzmeyer, de AFNIC, recomendó que se considerara el efecto que tendría un rechazo sobre aquellos que elaboraron y utilizan sistemas de nombres fuera del IETF. El rechazo en primera instancia de los que vienen al IETF a documentar su protocolo podría resultar en una pérdida de confianza en el organismo de estandarización. Luego de su intervención, escribió en la lista de correos que se había quedado "estupefacto de enterarme de que tenemos un 'equipo de diseño' para trabajar sobre la RFC 6761bis, cuando todavía no hemos logrado un consenso acerca de los problemas que existen con la 6761". Bortzmeyer está entre los que critican fuertemente la posibilidad de que se dé un salto hacia atrás en el proceso de reserva de nombres especiales.

En el polo opuesto se halla, por ejemplo, el presidente de la IAB, Andrew Sullivan, quien reaccionó intensamente durante la reunión del GT sobre DNSOP y definió algunas de las propuestas como "ataques contra la manera de funcionar del DNS". "Utilizar el espacio de nombres de dominio para subvertir el DNS es una mala idea", afirmó. Sullivan no ve por qué el IETF debería reservar nombres para los que están tratando de competir con los "modelos empresariales de los demás", y exhortó a que se separaran las propuestas y que fueran tratadas según correspondiera. A los que proponen un "nuevo sistema de identificación global, tengo que decirles, perdón, pero ya tenemos uno", le comentó a esta periodista.

Por otra parte, en un largo correo electrónico en la lista de correos del GT sobre DNSOP, Sullivan matizó sus comentarios acerca de las intenciones de los proponentes, y explicó por qué se opone a ciertos nombres:

> Entonces, así como .local marca algo para que sea buscado solo con el DNS, .onion y .exit marcan algo para que sea buscado solo dentro del enrutamiento de onion (o quizá, dependiendo del punto de vista, solo usando TOR). Pero otras de estas propuestas, como .bit, marcan un espacio de nombres y un protocolo asociado que compiten con el DNS. Es un universo paralelo de resolución de nombres que sirve para cualquier aplicación de la red. Mi argumento es que la segunda clase de nombres, básicamente, nos pone en la posición de aprobar registros de uso especial que constituyen, efectivamente, un ataque contra otros modelos empresariales (el de ICANN y el de los distintos Registros y registradores). Creo que impulsa al IETF hacia una batalla política para la que no está preparado, y esa es la razón por la que estoy en contra de estos registros.

La "batalla política" es una preocupación compartida por un número considerable de participantes en el IETF, como ilustra la discusión más amplia en la lista de correos de esta organización. De hecho, aparece como el tema principal en esa lista.

Se han hecho propuestas para mantener las reservas "técnicas" en una zona especial (como .alt o .external o, incluso, .ring). Los solicitantes se oponen a esta idea, porque los nombres que pidieron ya están en uso. Si .alt hubiera estado disponible hace años, alegó Grothoff refiriéndose a uno de los solicitantes, un proyecto podría haber considerado utilizarlo. Por otra parte, otros, como Bortzmeyer, se

oponen a cambiar las reglas ahora, en medio del juego.

Deshacerse de la 6761: la ocupación ilegal de .local sentó un mal precedente

Sin embargo, el Grupo de Trabajo parece estar eligiendo el camino de reabrir la 6761, según Suzanne Woolf, con un equipo de diseño de tres a cinco miembros que serán anunciados en breve por los presidentes del GT. Woolf es oficial de enlace con la Junta de ICANN (nombrada por el Comité Asesor del Sistema de Servidores Raíz) y miembro de la IAB. Afirmó que el equipo de diseño no tomaría ninguna decisión sobre una posible versión bis de la RFC, pero presentaría resultados de la evaluación de los problemas realizada por los miembros del GT durante el debate reciente. David Conrad, de ICANN, lo dijo sin rodeos: calificó las RFC 6761 y 6762 de "formalización de la ocupación ilegal del espacio de nombres", y afirmó que habían sentado un mal precedente.

El proceso de reserva es poco claro

En lo que podría considerarse como un comienzo del trabajo de diseño, Peter Koch, de Denic, y Alain Durand, de ICANN, analizaron cuidadosamente algunos de los temas a discutir.
Aun si no se cambia la RFC, las nuevas solicitudes pueden fracasar, argumentó Koch. Las solicitudes P2P, para empezar, no pudieron convertirse en documentos del IETF en vías de normalización (al revés de la RFC 6762 de .local). De acuerdo con Koch, las siete preguntas que los solicitantes deben contestar para poder reservar nombres especiales no servirían como justificación para reservar un nombre.

En primer lugar, varias cuestiones no estaban claras en la 6761:

- ¿Cuál es el proceso para conseguir una reserva? (Se necesita un documento que inicie el camino hacia la normalización.)
- ¿Quién decide? (¿El IESG [Grupo Directivo de Ingeniería de Internet], el GT sobre DNSOP, que, en realidad, no fue mencionado en el documento preliminar, o un GT especial constituido ad hoc?)
- ¿Qué se obtiene con la reserva? (¿Garantías respecto de la prevención de la fuga de datos? En el documento preliminar se menciona la expectativa de implementación por parte del público.)
- ¿Se necesita un proceso de eliminación?
- ¿El solicitante elegirá la cadena, o el IETF puede participar en la decisión?
- Relación entre el principio de "raíz única" y los nombres alternativos (pregunta de Sullivan)
- ¿Qué clase de coordinación se debe establecer con ICANN?
- ¿El IETF puede hacer algo más que analizar el protocolo?

Koch y Durand citaron literalmente de la Sección 3 de la RFC 6761, afirmando que el proceso crearía "un nivel más alto de reglas protocolares, por encima de la administración de ICANN de nombres asignables en la Internet pública". En esencia, este parece ser el principal miedo de muchos: que el IETF podría verse involucrado en las peleas vinculadas con las nuevas delegaciones de TLDs, con mucho dinero y abogados de por medio. No obstante, si el IETF ya está en una posición incómoda – ya que rechazar .onion después de .local queda mal – no rechazar .onion dificulta el rechazo de otros TLD P2P. Permanezcan atentos.

Elegir nuevas firmas para TLS y observar cuidadosamente la criptografía post-cuántica

Luego de las revelaciones de Snowden y de que el NIST admitiera la manipulación de ciertos procesos de cifrado por parte de la NSA, el Crypto Forum Research Group (CFRG) recibió el mandato de elegir

nuevos algoritmos de cifrado para TLS. Habiendo seleccionado Curve25519 y Goldilocks (Curve448) como nuevos conjuntos cifrados, el CFRG aún tiene otro "concurso de belleza" para el cual invitar propuestas de esquemas de firma. Al mismo tiempo, el GT decidió de manera unánime empezar a considerar algoritmos de cifrado post-cuánticos seguros. El CFRG sigue en la senda de convertirse en instancia alternativa para elegir la criptografía para la Internet pública, mientras que el NIST trata enérgicamente de no ceder control, como lo demuestran los debates en un taller reciente sobre criptografía de curva elíptica. El anuncio, realizado por un empleado del NIST, de que el Secretario de Comercio de EE UU acababa de firmar un nuevo hash Sha3 no ha recibido mucha atención en el IETF hasta ahora, según comentó un experto durante la sesión del CFRG.

Decisión rápida sobre los esquemas de firma

Durante la reunión del CFGR, se presentaron cinco propuestas para el nuevo esquema de firma: de Dan Brown e Ilari Liusvaara, de Dan Bernstein (Universidad de Illinois), de Tanja Lange (Universidad de Eindhoven) et al., de Mike Hamburg (Investigación en Criptografía de Rambus) y de Watson Ladd (presentada por Martin Thomson). Tanto Liusvaara como Bernstein presentaron comparaciones de las características principales de las propuestas, que abarcaron uso de los protocolos, codificación (por ejemplo, inversión, números aleatorios o interfaces de programación de aplicaciones e interfaces API no estándar), agregados, incluyendo la personalización, implementación de cortafuegos y capacidad de procesar por lotes, como describió Liusvaara.

Bernstein se refirió a una secuencia de comandos de python para permitir la comparación de los cinco candidatos, la cual, asimismo, permite monitorizar los cambios en las cinco propuestas. En la lista de correos, este investigador advirtió sobre el intento de "lograr un equilibrio criptográfico recortando todos los sistemas hasta el tamaño mínimo que puede lograr un nivel predeterminado de seguridad". Esta medida entraña el peligro de producir una deficiencia que permita el ingreso de atacantes.

Después de la presentación, el co-presidente del CFRG, Kenny Paterson, prometió que podía esperarse una decisión mucho más rápida acerca del esquema de firmas. La selección de la nueva cifra del Código de Corrección de Errores (ECC por sus siglas en inglés) había llevado más de un año, a pesar de que existía una vivencia de urgencia. Paterson afirmó que los esquemas de firma se decidirían, a más tardar, antes de la próxima reunión del IETF.

Criptografía cuántica: No la dejen para más adelante

El CFRG también acordó de manera unánime incorporar un tema de trabajo vinculado con la computación cuántica: votaron a favor de la propuesta de William Whyte de "criptografía barata que proteja de las computadoras cuánticas sin arruinar nada". Whyte, Director de Tecnología de Security Information, dijo que no estaba claro cuándo estarían disponibles las computadoras cuánticas, pero que sucedería mucho antes de los 30 años que se estiman habitualmente. Con estas computadoras, el RSA, las curvas elípticas y los algoritmos Diffie-Helman serían fáciles de decodificar. Según Whyte, pasar directamente a un nuevo conjunto de cifrados resistentes a las computadoras cuánticas podría resolver el problema, pero ni el CFRG empezó a hablar del tema, ni sería fácil de implementar. Propuso, en cambio, un "abordaje híbrido" que combine encriptación de clave pública/intercambio de claves que proteja de las computadoras cuánticas, y algoritmos ya existentes. El ejemplo que él promueve es el de los algoritmos NTRUEncrypt (patentados por su empresa), que fueron integrados al protocolo de intercambio de claves NTOR en un esfuerzo por brindar un sistema seguro para computadoras cuánticas para TOR. NTOR podría implementarse también con 25519, por ejemplo.

Algunas alternativas posibles a NTRUEncrypt son los sistemas de criptografía de clave pública seguros para computadoras cuánticas "Learning with Errors" y McEliece. Este último, sin embargo, tiene claves muy largas. Los datos sobre desempeño para NTRUEncrypt-NTOR son satisfactorios en términos de gastos generales para el cliente (que tiene que pagar la mayoría) y el enrutador. La patente existente fue recibida con alguna reserva en la sesión del CFRG. Otra implementación del concepto híbrido es una "extensión" de la TLS que incluya un "identificador híbrido de conjuntos cifrados seguro para computadoras cuánticas (QSH)" y "extensiones para claves públicas y textos cifrados seguros para computadoras cuánticas". Según Whyte, puede encontrarse un código ejecutable aquí. Nuevamente, se está usando NTRUEncrypt.

Whyte y la investigadora Tanja Lange respondieron preguntas acerca de la necesidad de impulsar la criptografía segura para computadoras cuánticas cuando los conjuntos cifrados ya existentes se siguen considerando seguros. La comunicación lograda con criptografía de última generación es susceptible a ataques de tipo "recolectar y después desencriptar" (*harvest-then-decrypt*). Lange afirmó que si la gente quería tener información delicada que siguiera estando protegida dentro de diez años, tendría que adoptar el nuevo sistema. Se refirió a un proyecto de la UE, Horizon 2020, de 3,9 millones de euros, que empezó en marzo. El NIST organizó su taller sobre ciber-seguridad en un mundo post-cuántico en abril. Whyte dio otro ejemplo práctico sobre la necesidad de ocuparse de la criptografía post-cuántica durante la plenaria de la IAB, vinculado con la comunicación de automóvil a automóvil y la seguridad que esta requiere, e indicó que los automóviles duran por lo menos una década.

DNS: "Privacidad bastante mala"

Según Haya Shulman, investigadora de la Universidad de Darmstadt, la privacidad del DNS es aún peor de lo que se cree. Shulman exploró ataques de canal lateral contra consultas de DNS que persisten incluso después de la implementación de DNS sobre TLS, y también cuestionó la introducción de TLS, debido a que muchos servidores no admiten TCP. A partir de mediciones en los primeros 50 mil dominios Alexa y en 568 TLDs, podría esperarse la presencia de obstáculos para la implementación de DNS sobre TLS en "por lo menos 38% de los servidores y 12% de los TLD". Por esta razón, Shulman pone en duda la eficiencia de DNS sobre TLS y de mecanismos similares, y recomienda la realización de nuevos estudios. La investigadora recibió el "Premio de investigación aplicada a las redes" del IRTF por este trabajo.

Los ataques de canal lateral sobre DNS y qué hacer para evitarlos

¿Ayuda acaso encriptar las preguntas y respuestas?, fue la reacción de Shulman a los mecanismos de privacidad que presentó brevemente (incluyendo la Curva DNS, DNSCrypt, DNS sobre TLS e IPSec oportunista). Con frecuencia, tener la dirección IP alcanza para suponer correctamente a qué dominio se accede. Esta suposición puede realizarse mediante la correlación de la dirección IP de destino en la consulta en el DNS, y los servidores de nombre de dominio. La coexistencia de dominios (hasta 500 para algunos servidores) puede enturbiar la imagen. Sin embargo, otros canales laterales ayudan a refinar la suposición, especialmente, el tamaño de la consulta y de la respuesta, la latencia entre la consulta y la respuesta u otros canales laterales más específicos, en particular, los "factores de dependencia en relación con la confianza transitiva".

El hecho de que un dominio a menudo tenga más de un servidor de nombres de dominio para permitir la redundancia y la resiliencia, y que los servidores de nombres de dominio, a su vez, estén configurados bajo distintos dominios, le brinda al atacante un gráfico de dependencias. Una vez que el atacante tiene una base de datos sobre estos factores de dependencia, puede emparejar dichos datos con

las consultas/respuestas y, así, eliminar el anonimato.

Durante el GT de DPrive, se presentó una posible respuesta a los ataques de canal lateral y a ese tipo de "toma de huellas digitales" de las consultas y respuestas en el DNS: el "relleno" – el agregado de bits a las consultas encriptadas (antes de la encriptación) – ayuda a desdibujar el tamaño de las consultas. Este fue presentado por Daniel Gillmor (EFF) en el GT sobre TLS como una opción para mejorar la privacidad de TLS, pero Alex Mayrhofer, de nic.at, sugirió que podría utilizarse también como alternativa para DNS sobre TLS. Como dijo Gillmor, todavía podría llevar algún tiempo implementar el relleno para la versión 3 de TLS, que está por elaborarse. No está claro si se implementará en TLS 1.2. Además, se mencionó el posible truncamiento debido al tamaño de las consultas "rellenadas" de DNS como un factor a considerar en relación con la seguridad.

Problemas con el DNS encriptado

La segunda medición de Shulman verifica en qué medida el DNS instalado está preparado para la encriptación. La investigadora señala varios problemas: la falta de interoperabilidad con la memoria caché podría resultar en costos generales de tráfico prohibitivos para los servidores, la encriptación podría ser incapaz de ocultar un servidor de autoridad detrás de un servidor recursivo y, finalmente, la capacidad del software instalado de admitir el protocolo TCP es un factor limitante.

Shulman informó acerca de una variedad de modos de falla, no solo en el caso del cliente, sino también en un número de servidores. Incluso algunos dominios populares se vieron afectados. Se refirió a 21 fallas fatales diferentes para las 50 mil páginas Alexa, y presentó una lista interesante de dichas fallas (con TCP) que afectaron a muchos servidores populares:

- Después de las negociaciones en TCP, la consulta en DNS recibe como respuesta RST+ ICMP(type=3, code=10), el servidor no puede responder (prohibido administrativamente), por ejemplo: edns-chtn.cht.com.tw 202.39.168.132
- Después de las negociaciones en TCP, la consulta en DNS recibe como respuesta ACK y luego RST, por ejemplo: gerek.accv.es 195.77.23.35
- El servidor sigue reenviando SYN+ACK, por ejemplo: ns7.utoronto.ca 162.243.71.42
- Después de las negociaciones en TCP, la consulta en DNS recibe como respuesta RST, por ejemplo: dns1.hessen.de 141.90.2.53
- Fluctuaciones de la ventana de TCP: SYN+ACK con ventana 0, luego SYN+ACK con ventana > 0 (vg., 4096), por ejemplo: beloit.edu 144.89.40.1
- Después de las negociaciones en TCP, la consulta en DNS recibe como respuesta múltiples pequeños segmentos, por ejemplo, segmentos de tamaño < 100 bits para una longitud de respuesta de 557 bits, por ejemplo: ns.CWRU.Edu 129.22.4.1
- Después de las negociaciones en TCP, el servidor envía SYN+ACK, y luego permanece en silencio, por ejemplo: cnsa.vita.virginia.gov 166.67.65.169

Como conclusión, afirmó Shulman, si bien la encriptación es "sin duda importante", sería beneficioso que la comunidad prestara más atención al flujo de trabajo en las configuraciones de infraestructura existentes porque "cuál sería la ventaja de adoptar algo que después no funcione". La investigadora anunció que el próximo paso en su investigación sería intentar diferenciar entre problemas "normales" de conectividad, por un lado, y ataques de degradación contra la TLS. Pronto presentará un trabajo sobre este tema.

Grupos de Trabajo y BoFs

DPRIVE

A pesar de las opiniones bastante escépticas de Haya Shulman sobre la eficiencia de los esfuerzos de encriptación en DNS (véase "DNS: Privacidad bastante mala"), DPRIVE está avanzando. La publicación del documento sobre privacidad en DNS es inminente (está en la cola del Editor de RFCs desde hace varias semanas).

Los presidentes del GT y los autores del documento básico acerca de DNS sobre TLS (Allison Mankin et al.) esperan que llegue a la etapa de última llamada en los próximos meses. Algunos elementos que se agregarán al documento preliminar son TLS 1.2 o mejor (sin base instalada) y una referencia a la RFC 7525 (BCP 195 "Recomendaciones para el uso seguro de TLS y DTLS"). Una discusión fundamental que todavía no está resuelta se vincula con la pregunta de si debería usarse un nuevo puerto, en vez de Start TLS, para establecer la conexión segura. Aun cuando es más fácil de implementar, varios miembros del GT afirmaron que es necesario tener mejores datos y un análisis de amenazas. El GT no acordó una respuesta final a esta pregunta. Si bien se consideró que el documento preliminar de evaluación era importante, no se le prestó tanta atención.

Hay varios problemas comunes a DNS sobre TLS y a DNS sobre DTLS, que espera evitar los problemas clásicos de TLS (bloqueo de encabezado de línea) y, a la vez, ofrecer una privacidad aumentada utilizando UDP. Según Dan Wing, que presentó el documento preliminar, las ventajas son también su uso amplio en protocolos como WebRTC y la velocidad en la reanudación de las sesiones (con DTLS 1.3, las sesiones podrían empezar con tiempo 0 de ida y vuelta, un dato que se ha utilizado para promocionar QUIC, el protocolo de transporte alternativo propuesto por Google, como puede verse más abajo). Salvo los inconvenientes con anycast, que son específicos para DNS sobre DTLS, la mayoría de los problemas son comunes a ambos protocolos: el bloqueo de tráfico encriptado sobre el puerto 53, la autenticación del servidor DPRIVE y los ataques de degradación. Estos últimos también constituyen una de las preocupaciones mencionadas por Haya Shulman (véase más arriba).

DNS sobre DTLS ya fue adoptado como documento preliminar del GT. No hubo mucho interés en otra solución presentada: IPSEC. En lugar de realizar cambios potencialmente complicados al DNS, afirmó Paul Wouters, de Redhat, IPSEC es una opción para encriptar todo el tráfico (VPN). El documento preliminar está siendo elaborado actualmente en el GT de IPSECME (Mantenimiento de la Seguridad y Extensiones de IP) (véase aquí).

DNSOP

Además del debate conflictivo acerca de cómo abordar la política de reserva de nombres especiales (véase más arriba), el GT sobre DNSOP debatió intensamente sobre aspectos del uso de TCP para DNS. A la vez que respalda los documentos preliminares sobre privacidad en DPRIVE (como se informó anteriormente), este protocolo está motivado por la oferta de protección contra falsificaciones (*spoofing*) y ataques de amplificación, así como por el avance generalizado hacia mayores tamaños de las respuestas en DNS (DNSSEC e IPv6). Presentado por Sara Dickinson, una de las co-autoras del documento preliminar sobre DNS sobre TLS, el documento apunta a hacer que TCP sea una parte "obligatoria" de la implementación completa del protocolo de DNS. No obstante, el GT reconoció que es difícil imponer conductas, especialmente para un protocolo como DNS, que existe desde hace mucho tiempo. Geoff Huston advirtió que es necesario ocuparse también del riesgo de las conexiones inactivas de TCP.

Se supone que EDNS-TCP-Keep Alive, cuyo documento resucitado fue presentado también por

Dickinson, indica un tiempo variable de desconexión por inactividad para las conexiones de TCP, y ayudará a equilibrar las proporciones del tráfico que corresponden a UDP y a TCP. Los servidores podrían indicar lo que esperan, y los clientes elegirían mantener la conexión en funcionamiento por más tiempo. Los beneficiarios potenciales serían los recursivos validadores y TOR.

Finalmente, se discutieron posibles abordajes para una recuperación segura de los anclajes de veracidad durante el periodo posterior al traspaso de la KSK. Joe Abley afirmó que la recuperación y, asimismo, un mecanismo estándar de arranque automático de los recursivos validadores seguían siendo aspiraciones en relación con el próximo traspaso. Abley informó que el equipo de diseño para el traspaso de la KSK pronto publicará su propuesta para que la analice la comunidad. Además, sugirió resucitar documentos más antiguos sobre la recuperación de anclajes de veracidad y arranque de los recursivos validadores. Surgieron preguntas acerca de por qué estos serían necesarios cuando existe la RFC 5011, que debería ser impulsada en su lugar. También recibió peor acogida una rápida propuesta de Warren Kumari, de Google, quien pidió un posible mecanismo de señalización que avise cuando se produzca el traspaso de la clave.

DANE: Incorporarlo a la infraestructura básica

El GT sobre DANE sigue trabajando para que este protocolo sea más utilizable en la validación y autorización de distintas aplicaciones clientes. Se presentaron dos propuestas. La primera describe una "extensión de TLS para el transporte de un conjunto de registros de DNS que está serializado con las firmas DNSSEC necesarias para autenticar ese conjunto de registros". Serializar los controles permite al cliente de TLS realizar la autenticación DANE de un certificado de servidor de TLS sin emprender búsquedas adicionales de registros de DNS. De este modo, la latencia es menor, se evita la interferencia de dispositivos intermedios y existe la opción de permitir la autenticación de la capa de enlace. Los usuarios serán navegadores de Web, servicios de voz sobre IP y de XMPP u otros clientes de TLS que no quieran o no puedan buscar registros de DANE.

La segunda propuesta está dirigida a las aplicaciones de TLS que ya usan la autenticación DANE de servidores y podrían proceder a autenticar clientes utilizando el mismo mecanismo. Según los autores, Victor Dukovni (de Two Sigma) y Shumon Huque (de VeriSign), se trata de una actualización de la RFC 6689. Algunos de los patrones de diseño podrían ser beneficiosos para el diseño en la Internet de las cosas, que utiliza esta forma de autenticación para objetos materiales grandes identificados. Según esta modalidad, grandes redes de objetos materiales identificados por nombres de DNS pueden autenticarse a sí mismos con un dispositivo de gestión centralizada.

Los co-presidentes del GT sobre DANE propusieron permitir una zona/etiqueta conjunta para el OpenPGP (que está siendo evaluada por los Directores de Área) y el documento preliminar de DANE SMIME (que aún está siendo considerado). Además, dos documentos del grupo DANE están esperando en la cola del editor de las RFC: Dane-smtp-con-dane y dane-srv.

QUIC: ¿mucho mejor que el TCP?

Desde la aparición en abril de un posteo en un blog de la página Web de Google sobre el interés de la empresa en estandarizar QUIC, ha habido rumores en relación con ese protocolo de transporte. En un Bof en el Bar [reunión paralela que no forma parte del programa oficial] muy concurrido (entre 250 y 300 personas), Ted Hardie, de Google, aclaró que, por el momento, la empresa no estaba intentando conformar un grupo de trabajo. En cambio, como dijo uno de los autores del protocolo a esta periodista, quiere mantener QUIC bajo su propio control (un GT resultaría en la transferencia de dicho control al

IETF) y realizar más experimentos.

Según Jana Iyengar, uno de sus creadores, QUIC se parece a "TCP más TLS más SPDY sobre UDP". El principal objetivo de este protocolo es la velocidad: posibilita que haya 0 tiempo de ida y vuelta y, además, incluye elementos nuevos, como un número de identificación en lugar de la dirección de IP que permite que se mantenga la conexión al moverse entre distintas redes. Lo bueno del TCP, declaró Iyengar, es que puede actuar como plan alternativo y, así, posibilita que los creadores de QUIC experimenten. Esta es también la razón por la cual Google no quiere estandarizar este protocolo, sino mantenerlo aparte, para que pueda superar al TCP. Si bien no solicitó su estandarización, la empresa pidió su implementación por parte de los participantes en el BoF. Christian Huitema, de Microsoft, dio una presentación sobre dicha implementación.

Sin embargo, la ligereza de QUIC tiene algunos aspectos negativos. Daniel Kahn Gillmor advirtió que, si bien trabaja siempre con encriptación, la identificación que permanece activa a través de las redes por las que navega un usuario permite un perfecto seguimiento. Tanja Lange, experta en encriptación de la Universidad de Eindhoven, advirtió acerca de los ataques de repetición que resultan del 0 tiempo de ida y vuelta, que deben ser resueltos. Además, uno de los directores de área del IETF dijo que la corrección de errores sin canal de retorno (FEC por sus siglas en inglés) todavía sigue siendo experimental.

EPPEx
EPPExt

Como muchas de las extensiones al EPP (Protocolo de Aprovisionamiento Extensible) de la primera ronda ya están en la etapa de última llamada o cerca de ella, el GT sobre Extensiones al EPP se está preparando para analizar una nueva ronda de extensiones. Una breve discusión del Acta Constitutiva confirmó que el GT seguirá estando disponible para la discusión de nuevas extensiones, que serán registradas en el registro de extensiones al EPP de la IANA. Se las puede registrar con fines informativos, siempre que exista una especificación publicada que haya sido revisada por un o una experta designada. El GT evaluará aquellos documentos que quieren convertirse en estándares de Internet. Se puede intentar combinar funciones similares del EPP.

Los presidentes ofrecieron una lista de posibles candidatas para extensiones del EPP. Rik Ribbers (SIDN) presentó una extensión para un relevo seguro de claves en DNSSEC como una de las últimas propuestas de la primera ronda, y se acordó que esta estaba lista para la última llamada. El relevo genérico para transferir claves de DNSSEC de manera segura durante un cambio de proveedor está fuera del ámbito de discusión de este GT.

Ning Kong (CNNIC) presentó dos documentos sobre el manejo y el mapeo de distribuidores como los primeros dos nuevos documentos. Para ver la lista de nombres de los documentos preliminares, pueden hacer click aquí: https://tools.ietf.org/wg/eppext/

Novedades del IETF

Premio Postel

Rob Blokzijl, miembro fundador de RIPE (Redes de IP Europeas) y su presidente durante 25 años, recibió el Premio Jonathan Postel de 2015. Blokzijl, físico de profesión, se involucró con Internet cuando su jefe en el Instituto Nacional de Física Nuclear y de Altas Energías (NIKHEF) le pidió que facilitara su trabajo en Internet con CERN, la organización europea de investigación en energía nuclear,

en los años 80. Blokzijl también tuvo un rol protagónico en la creación de RIPE NCC, el registro regional europeo, y en la fundación del Intercambio de Internet de Amsterdam (AMSIX), y fue miembro de la primera Junta de ICANN en representación de la Organización de Soporte de Direccionamiento (ASO por sus siglas en inglés) en 1999. En su discurso de aceptación, reconoció que un área que él había considerado como puramente técnica ha cambiado, e interactúa ahora con la política. Blokzijl es el 17º ganador del premio.

Derechos de propiedad intelectual de la IANA

El IETF canceló una reunión del GT sobre el plan de la IANA, a cargo de analizar su traspaso a un organismo de control multipartito y totalmente privado. Según el presidente del IETF, Jari Arkko, se pensó que no había nada nuevo para informar. El tema, algo controvertido, de los derechos de propiedad intelectual y del nombre de dominio de la IANA se trató solo brevemente durante la plenaria administrativa del jueves. El nuevo presidente de la Fundación IETF, Benson Schliesser, de Brocade (quien reemplaza a Tobias Gondrom, ahora presidente del Comité de Supervisión Administrativa del IETF, o IAOC), acaba de volver a confirmar que la Fundación "estaría dispuesta a ser titular de los derechos de propiedad intelectual vinculados con la función de la IANA, incluyendo la marca registrada IANA y el nombre de dominio IANA.ORG". La propuesta de traspaso del GT, que afirma que **"ICANN le otorgará a la PTI [IANA post-transición] una licencia exclusiva, libre de pago de derechos, pagada en su totalidad y válida en todo el mundo para utilizar la marca registrada de la IANA y todas las marcas registradas vinculadas con ella en relación con las actividades del PTI bajo el contrato entre ICANN y el PTI** ", no fue debatida en la reunión de Praga. Arkko le dijo a esta periodista que había una incompatibilidad vinculada principalmente con CRISP ("Propuesta consolidada de los RIR para la supervisión de las funciones de la IANA").

El próximo IETF se realizará en Yokohama del 1 al 6 de noviembre de 2015.