Informe sobre IETF 110

Reunión virtual

8 al 12 de marzo de 2021

Los contenidos del informe fueron producidos por CENTR y traducidos 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

lactld

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

Contenidos

Introducción

El presente informe compila una serie de artículos y entrevistas publicados CENTR acerca del IETF110, los últimos desarrollos en torno a la privacidad en el DNS, y el despliegue y automatización de las DNSSEC.

Novedades de la reunión IETF110

Por Monika Ermert

Por cuarta vez consecutiva, el Grupo de Trabajo de Ingeniería de Internet (IETF) se reunirá de manera virtual durante esta semana (del 8 al 12 de marzo). Esta modalidad no impidió que el organismo de estandarización de Internet lleve a cabo más trabajo en el área del DNS. Lo siguiente es una breve descripción de la abultada agenda y algunos aspectos destacados para los participantes interesados.

Más acerca de la privacidad en el DNS

Mejorar la privacidad en el DNS ha sido tema de agenda desde hace varios años, y aún queda mucho trabajo por hacer. El día de hoy, el Grupo de Trabajo (WG) de DPRIVE debatirá un tema que ha estado inactivo desde hace un tiempo: el cifrado del tráfico desde el resolutor recursivo al autoritativo en el árbol del DNS.

Por primera vez, se debatirá añadir seguridad criptográfica en la segunda pierna de la jerarquía de resolución del DNS, según explica Vladimir Cunat, de CZ.NIC. Los servidores TLD parecen ser los puntos predominantes para tener en cuenta la privacidad, "ya que mucho de su tráfico contiene necesariamente los nombres de los sitios web a los que se accede". Apple, Mozilla, Google y Cloudflare presentarán un *draft* sobre la manera en que los resolutores autoritativos pueden señalar que son compatibles con el cifrado. Tal documento se debatirá junto con la propuesta sobre el cifrado de la ruta entre el resolutor recursivo y el autoritativo, elaborada por Paul Hofmann, de ICANN, y Peter Van Dijk, ingeniero en PowerDNS.

El WG de DPRIVE también profundizará sobre la idea de desvincular la identidad del cliente del contenido de sus solicitudes a través del Oblivious DNS sobre HTTPS (ODoH). El ODoH se introdujo, en principio, en el WG de Adaptive DNS Discovery (ADD), pero ADD ahora se centrará en el descubrimiento de resolutores.

Cabe mencionar que las solicitudes "oblivious" (desentendidas) han despertado un interés especial en los expertos de HTTP. Por ello, Martin Thomson, de Mozilla, le pedirá al WG de SecDispatch que considere su *draft* sobre Oblivious HTTPS el jueves (16:00 h UTC). Hacer que las solicitudes sean "desentendidas" en el DoH sobre HTTPS requiere que un proxy acepte la solicitud de un cliente de contenido/nombres. El proxy no observará el contenido de las solicitudes, ya que

estarán cifradas, y las enviará al resolutor sin información adicional sobre el solicitante.

El WG de DNS Operations se reunirá el jueves a la tarde e intentará impulsar una serie de *drafts* existentes, en particular sobre las zonas de catálogo del DNS y trabajo adicional sobre las DNSSEC. Manténgase al tanto con el Grupo de Investigación de Mediciones y Análisis para los Protocolos (MAPRG), que ha llevado a cabo varias charlas de investigación relacionadas con el DNS (archivadas para la posteridad).

Un nuevo transporte

Se publicaron dos series de RFC muy importantes justo antes de la IETF110, la serie de RFC de WebRTC y la versión uno del nuevo protocolo de transporte cifrado basado en UDP: Quic. Este último ciertamente también abre paso a otra idea relacionada con el DNS: el DNS sobre Quic. La propuesta de Christian Huitema ha quedado en espera durante un tiempo, pero puede que se adopte en el WG de DPRIVE el martes. Si es así, cambiará una vez más la ecuación para lograr un DNS con mejor privacidad.

Otros temas por considerar

Para quienes tengan tiempo, hay otros temas muy interesantes en la agenda. La reunión del WG de Registration Protocol Extensions es imperdible para muchos expertos en registros. Esté atento a la BoF sobre Dane Authentication para el endurecimiento de servicios (Danish), que quizás finalmente prepare el terreno para Dane, la alternativa no tan querida a WebPKI.

Para quienes se pregunten sobre el futuro de las redes, puede ser interesante toda el área de redes de aplicación específica. Se está intentando constituir un WG para esto. ¿Qué beneficio aportará para la privacidad? Tommy Pauly, miembro de la IAB e ingeniero en Apple, y Lorenzo Colitti, de Google, (WG de IntArea, viernes por la tarde) responderán esta pregunta, y un *draft* del presidente de la IAB, Jari Arkko, profundizará sobre las consecuencias del desarrollo, también desde la perspectiva de la privacidad.

¿La indirección del tráfico es lo que se viene en la privacidad en el DNS y otros ámbitos?

Por Monika Ermert

Luego del Oblivious DoH, se le presentó al Grupo de Trabajo de Ingeniería de Internet (IETF) el Oblivious HTTP y la informática confidencial (*confidential computing*) durante la reunión IETF110. Básicamente, estos mecanismos propuestos intentarán proteger la información de los usuarios contra recolectores de datos indeseados.

Desarrolladores de Apple, Fastly y Cloudflare propusieron un estándar "Oblivious DNS" u "Oblivious DNS sobre HTTPS (ODoH)" como respuesta ante las reacciones contra el DoH. La implementación del DoH original de Mozilla suscitó muchas preocupaciones sobre sus efectos de concentración. Se supone que el Oblivious DoH debe mitigar el riesgo de la recopilación de datos por parte de un resolutor centralizado.

Al poner un proxy entre el usuario y el resolutor DNS, el ODoH hará que las solicitudes de dominios sean anónimas. Únicamente el proxy conocerá la dirección IP del usuario, pero no verá el contenido de la consulta DNS, ya que viaja de ida y vuelta en forma cifrada. El resolutor se limitará a responder las solicitudes, sin saber quién las hizo.

Cloudflare, al ser el proveedor criticado y centralizado para la implementación inicial del DoH de Mozilla, se apresuró a implementar el ODoH a finales del año pasado, en sociedad con PCCW, SURF y Equinix, que trabajan como proveedores de proxy independientes.

Chris Wood y Tommy Pauly, ingenieros de Apple, ahora esperan que se adopte el *draft* del ODoH. Según Pauly, Apple tiene la intención de ser compatible con el ODoH en el futuro.

No obstante, el WG de DNS Privacy Group (DPRIVE) vaciló, mencionando las implementaciones existentes que están en marcha y una segunda versión del concepto de "oblivious" que ya se ve en el horizonte, al que Wood mismo hizo referencia durante la reunión.

La generalización del concepto de "oblivious"

En lugar de limitar el concepto de "oblivious" al DNS sobre HTTP, Martin Thomson (Mozilla) y Wood tomaron la iniciativa para la generalización del concepto de "oblivious".

Como en el concepto del ODoH, la indirección es el mecanismo que previene que los servidores recopilen solicitudes y las relacionen con perfiles de usuarios. Un servidor proxy oculta la dirección IP del usuario y la solicitud se cifra para ocultarse

del proxy. El trabajo se basó, en gran medida, en el concepto del ODoH, pero se expresó el deseo de generalizarlo para que abarque más que las consultas DNS, según dijo Thomson en la sesión de SecDispatch.

Según Thomson, OHTTP está adaptado para casos de uso transaccionales, atómicos y breves, como las solicitudes DNS. Observó que era menos oneroso que la navegación en Tor, pero que ofrecía una protección similar. Remarcó que Mozilla también esperaba usar la herramienta para consultas de telemetría, para lo que no se buscaba ningún dato de usuario individual.

Hay más trabajo en marcha en el IETF sobre el uso de proxies. Muchos participantes reconocieron la necesidad de mapear el trabajo y explicar cómo este está relacionado. David Schinazi (Google) hizo referencia a la estandarización actual en el WG de Masque, en particular. Dijo que, sin embargo, OHTTP aborda un caso de uso especial al centrarse en solicitudes breves. La opinión de Schinazi es que las conexiones duraderas, la navegación web y la construcción de sitios web enteros, por otro lado, se abordan mejor con Masque.

Al igual que el DoH y, en menor medida, el ODoH, OHTTP recibió un rápido consenso para avanzar. Los participantes del IETF pueden contar con que se cree un WG de OHTTP próximamente.

Los próximos pasos hacia la privacidad en el DNS

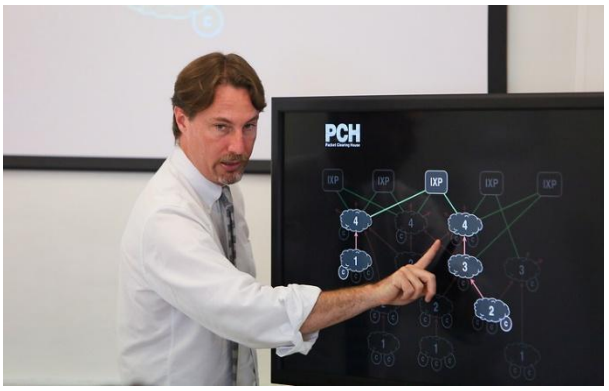
La tendencia general de permitir que los usuarios busquen recursos de manera anónima se evidencia una vez más en otro trabajo presentado en la IETF110. El expresidente del IETF e ingeniero de Ericsson, Jari Arkko, le dijo al WG de DNS Operations que, con el avance hacia el cifrado de las comunicaciones DNS y el ocultamiento de los metadatos de las consultas, ya se podían ver los próximos pasos hacia la privacidad. Los datos en reposo, según Arkko, deben ser cubiertos para evitar filtraciones de los resolutores, ya sea por accidente o debido a intenciones comerciales o maliciosas.

En lugar de una solución con proxy, Arkko presentó una propuesta que considera un entorno de ejecución confiable (TEE) como método para evitar la recopilación de datos en los resolutores. Si las consultas DNS se hacen dentro del TEE integrado al hardware, hasta los operadores de la nube podrían quedar fuera de la resolución. Un TEE de buen funcionamiento debe ofrecer la comprobabilidad de sus características, la integridad del código y la confidencialidad de los datos. Aquí se necesita la confianza de la misma manera que en los proveedores de proxy.

Si bien algunos participantes no creen que la informática confidencial se convierta en una operación del DNS, Arkko está seguro de que no es cosa del futuro. Según su *draft*, ya se están ofreciendo algunos TEE, por ejemplo, por parte de Intel (Software Guard Extension). Arkko anunció su intención de experimentar su uso durante la próxima hackatón del IETF en julio del 2021.

Privacidad en el DNS, cumplimiento de la ley y Quad9: una conversación con Bill Woodcock

Por Gurshabad Grover



Quad9 es un servicio gratuito del Sistema de Nombres de Dominio (DNS) que se centra en la privacidad y la seguridad. En febrero del 2021, la empresa se reconstituyó en Suiza para brindar a los usuarios garantías de privacidad aun más fuertes. La mudanza estuvo facilitada por SWITCH, miembro de CENTR y registro de los dominios de nivel superior .ch y .li. Para hablar sobre la mudanza y la privacidad en el DNS en general, CENTR entrevistó a Bill Woodcock, presidente del Consejo de Fundación de Quad9. El texto de la entrevista se editó levemente en pos de la brevedad y la claridad.

GG: En términos de privacidad para los usuarios de Quad9, ¿qué implica la mudanza de la organización a Suiza? ¿Ha habido otros cambios simultáneos en las políticas o prácticas de privacidad en Quad9?

BW: Esta mudanza tiene dos aspectos: nuestras políticas de privacidad (lo que nos comprometemos a hacer) y la ley aplicable (lo que la autoridad gobernante se compromete a hacernos cumplir). Esta última es mucho más importante que la primera: si una política de privacidad no está alineada con su cumplimiento legal, no sirve de nada ni ofrece protección real. Ese ha sido el problema con las empresas de tecnología que se esconden detrás de la jurisdicción de la Corte Federal de California del Norte de los Estados Unidos, donde el cumplimiento de las políticas de privacidad es plenamente voluntario. Por ello, las empresas estadounidenses se escudan de la responsabilidad ante sus usuarios y la sociedad, y esto produjo el infierno distópico hiperlibertario en el que estamos viviendo ahora, mientras se alientan horribles crímenes de odio y violencia. De esto se trata, por ejemplo, el llamado a la acción de Christchurch (conocido en inglés como Christchurch Call).

Fundamentalmente, nos mudamos a Suiza para salirnos de las fronteras de la jurisdicción de los EE. UU. y ubicarnos en un lugar donde la ley de rendición de cuentas fuera la más fuerte que pudiéramos encontrar. Cuando teníamos dirección en los Estados Unidos, nuestro cumplimiento de las políticas de privacidad era voluntario, como lo es el de cualquier empresa estadounidense. Al domiciliarnos en un país de la UE, estaríamos sujetos al Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) y a las sanciones

civiles que se aplicarían en caso de violación del GDPR en relación con un ciudadano de la UE. Sin embargo, en Suiza, se aplican sanciones penales si violamos la ley de privacidad suiza en relación con cualquier persona, en cualquier lugar del mundo. Realmente, esta es la mejor opción de ubicación para lo que queríamos: la protección legal más fuerte posible para todos nuestros usuarios, sin importar su país de ciudadanía o residencia.

Quad9 siempre estuvo en cumplimiento con el GDPR, y la ley de privacidad suiza es equivalente al GDPR en sus protecciones. La diferencia que aporta esta mudanza yace en la exigencia de cumplimiento de las leyes. Esto quiere decir que nosotros mantenemos los mismos altos estándares de nuestras políticas y prácticas de privacidad, pero ahora nuestra adherencia a ellas está respaldada por la envergadura de la ley suiza.

En el sitio web de la organización, he intentado compilar algunos elementos fundamentales de hallazgos jurídicos que explican la manera en que la ley suiza se aplica a Quad9 y el fundamento de estas protecciones para los usuarios. Todo esto se puede consultar en https://www.Quad9.net/service/privacy/.

GG: ¿Qué deberían saber los usuarios sobre la estructura de gobernanza de Quad9?

BW: Quad9 cuenta con un Consejo de Fundación de cinco representantes de partes interesadas: uno de la industria, uno del sector sin fines de lucro, uno de la comunidad técnica de Internet, uno del sector de investigación académica, y uno del gobierno.

GG: ¿Cómo recauda fondos Quad9? ¿Cómo se sustenta?

BW: Quad9 recibe financiamiento puramente de donaciones: la mayoría en especie, en lugar de en efectivo. La mayoría de estas donaciones consisten en espacio, electricidad, servidores y ancho de banda en el centro de datos. Nuestra base de donantes es amplia y diversa, y crece continuamente cada año.

GG: En los últimos años, ha habido una ola de adopciones de protocolos de DNS cifrado. El DNS sobre TLS (DoT) se estandarizó en el 2016. Si bien el DNS sobre HTTPS (DoH) se formalizó recién en 2018, su popularidad creció exponencialmente gracias a las presiones de grandes empresas tecnológicas y redes de distribución de contenidos (CDN), como Google y Cloudflare. Quad9, como sabemos, se convirtió en el primer resolutor en ofrecer estos protocolos. ¿Qué piensa del desarrollo y el despliegue de tales protocolos?

BW: Quad9 fue, de hecho, el primer resolutor que ofreció el DoT. El DoT es un protocolo excelente, que aplica TLS, un paquete criptográfico conocido, al DNS de manera directa, dándoles a los usuarios el beneficio de la confidencialidad en sus consultas en vuelo. El DoT no incorpora nuevas vulnerabilidades en comparación con sus predecesores.

El DoH, por otro lado, es como un caballo de Troya. Se introdujo mucho después que el DoT y tiene el efecto de debilitar la privacidad, en lugar de fortalecerla. El DoH facilita el "*fingerprinting*" (identificación) de los usuarios mientras se mueven entre distintas ubicaciones, lo que permite que la parte en el otro extremo de la conexión correlacione consultas DNS que, de otro modo, no están relacionadas y las una en un expediente único que identifica a ese usuario y su uso de Internet. Además, el DoH permite violaciones flagrantes a la neutralidad de la red cuando un operador de DNS también funciona como operador de CDN.

También brindamos compatibilidad con DNScrypt, un protocolo razonable que nunca pasó por el proceso de estandarización abierta.

GG: Mozilla también ha estado en la primera línea para el despliegue del DoH. Para asegurar que los usuarios de Firefox reciban opciones de servicios DNS que brinden ciertas garantías mínimas de privacidad, se ha lanzado un programa de Trusted Recursive Resolvers (Resolutores Recursivos de Confianza). ¿Qué piensa de su participación y de este programa?

BW: Creo que las motivaciones de Mozilla son buenas, pero las desventajas del DoH son tan preponderantes que es muy difícil que esto se haga correctamente y de manera segura. Creo que se dieron cuenta de eso, y que se evidencia en la manera en que están haciendo un esfuerzo honesto, ya que han vuelto al punto de partida y han solicitado participación pública antes de seguir adelante. Además, deben encontrar una manera de hacerlo en cumplimiento con el GDPR —a diferencia de su actual esfuerzo— para los ciudadanos europeos.

GG: ¿Unirse al programa está en los planes de Quad9?

BW: Hace más de dos años estamos negociando el contrato con Mozilla sobre este tema.

GG: Además de la privacidad, Quad9 también se ha comprometido públicamente a atenerse a un marco de derechos humanos amplio. ¿Qué piensa del compromiso de la organización respecto a la libertad de expresión y al derecho a buscar información? En particular, ¿en qué se basa la decisión de mantener como opción predeterminada de Quad9 el servicio que filtra respuestas DNS?

BW: El servicio de filtrado del DNS es opcional, y protege exitosamente a las personas de más de 140.000.000 infecciones de *malware* a diario. Trabajamos para cumplir tres objetivos: la privacidad, la seguridad y el rendimiento. Al proteger a las personas del *malware* y el *phishing*, Quad9 está cumpliendo su compromiso de brindar seguridad, y esa es la razón principal por la cual los usuarios recurren a nosotros. Tenemos políticas de derechos humanos claras, y aún no hemos recibido ninguna queja sobre las políticas ni la implementación de estas, pero siempre buscamos mejorar, así que recibimos con agrado todas las sugerencias que tengan las personas en relación con lo que se pueda mejorar.

GG: Algunas investigaciones recientes de CensoredPlanet sugirieron que es probable que los servicios de filtrado del DNS estén bloqueando contenido inofensivo (parece que no ha habido pruebas sobre esto en Quad9). ¿Quad9 monitorea la exactitud y la precisión de sus sistemas de filtrado?

BW: Sí, lo hacemos. También analizamos todos los informes de falsos positivos que nos llegan. Actualmente, tenemos una tasa de menos de un falso positivo en 600.000, con un promedio de 3,4 millones de dominios de *malware* y *phishing* bloqueados en todo momento, y una tasa de cancelación de aproximadamente 300.000 por día. Podríamos brindar una protección del 100 % simplemente bloqueando todo, a cambio de una tasa de falsos positivos de 1:1. O podríamos no proteger a los usuarios, y no tener ningún falso positivo. Se trata de un ejercicio de equilibrio, y lo que hemos logrado hasta ahora es una tasa de éxito del 98 % en la protección contra *malware*, con una tasa de falsos positivos de 1:600.000. Como dije antes, estamos constantemente intentando mejorar.

GG: Y en caso de que se produzcan bloqueos excesivos, ¿piensa que hay tensión entre la opción predeterminada (el servicio de filtrado) y la libertad de expresión?

BW: No. No quiero sonar simplista. En cinco años, nadie ha planteado problemas de libertad de expresión. Quienes distribuyen *malware* a menudo denuncian que sus dominios son un falso positivo, y a veces suben contenido para camuflar el *malware*, pero los descubrimos rápidamente.

Si alguien realmente quiere recibir *malware*, pueden usar nuestro servicio sin bloqueo. En cualquier momento dado, la cantidad de usuarios que está usando el servicio sin bloqueo es menor al 1 %. Generalmente, lo usan para acceder a sitios que han implementado incorrectamente las firmas DNSSEC, no porque quieran recibir *malware*.

Nuestro bloqueo no se basa en el contenido. A menudo recibimos solicitudes en relación con *spam* específico, bloqueo de anuncios y opciones “para toda la familia”, pero otras personas también llevan a cabo estas acciones, y nosotros tenemos recursos limitados, así que nos atenemos a lo más importante y que nadie más hace correctamente: filtramos *malware*.

GG: Parece que no es posible hacer una consulta a un resolutor de validación de DNSSEC mientras no se usa el servicio de bloqueo de *malware* de Quad9. ¿Hay algún motivo específico para que esto sea así o algún plan para que esto cambie?

BW: Existe un gran costo para el despliegue global y la compatibilidad de otra combinación de funciones. Muy pocas veces se han presentado solicitudes de un servicio de validación de DNSSEC sin filtrado. El costo de oportunidad de implementar toda una infraestructura superpuesta para dar soporte a algo que un puñado de personas piden quitaría recursos del servicio principal, el cual usa y necesita el restante 99,9998 % de las personas. Aun si invirtiéramos un gran monto en la compatibilidad para esta combinación de funciones, no se sabe si se

usaría significativamente. De todas formas, recibimos con gusto todos los comentarios.

GG: Gracias, Bill. Recomiendo, desde mi propia experiencia, el servicio del DNS de Quad9. Valoro la mudanza a Suiza, el compromiso de respetar la privacidad de los usuarios, y la transparencia acerca de las políticas y las decisiones de la organización. Gracias por tu tiempo y tus perspectivas. ¡Mis mejores deseos!

Despliegue y automatización de las DNSSEC: una entrevista con Ulrich Wisser

Por Gurshabad Grover

Objeto de debate desde la década de 1990, las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) añaden autenticidad a los registros DNS. Para comprender el estado actual del despliegue de las DNSSEC, entrevistamos a Ulrich Wisser, quien trabaja en The Swedish Internet Foundation, un miembro de CENTR que administra el dominio de nivel superior .se. También hablamos sobre un *draft* de coautoría de Ulrich Wisser que propone un algoritmo y un protocolo para automatizar las operaciones para las DNSSEC de múltiples firmantes. El texto de la entrevista se editó en pos de la brevedad y la claridad.

GG: La adopción de las DNSSEC en el mundo aún es más baja que lo que se esperaba en general. ¿Qué impidió el despliegue de las DNSSEC?

UW: Las herramientas disponibles para los servidores DNS autoritativos han sido bastante malas. Sin embargo, a lo largo de la última década, mejoraron al punto tal que las DNSSEC ahora son una opción “sí/no” en la configuración de dominios.

Del lado del resolutor, a menudo escuchamos que la resolución podría fallar con las DNSSEC. Pero, en Suecia, ni siquiera los ISP más grandes pueden recordar un solo caso en el que se hayan tenido que deshabilitar las DNSSEC para un dominio.

Uno de los mayores problemas en la adopción de las DNSSEC sigue siendo el mismo de casi toda la tecnología de seguridad: los clientes no las piden. Los vendedores de dominios están en un negocio de bajo margen, por lo que no gastarán dinero en algo que crean innecesario. Eso es entendible, pero no deja de ser frustrante.

GG: En la lista de correo electrónico de las operaciones del DNS en el IETF, mencionó que .se tiene una alta penetración de DNSSEC (aproximadamente del 50 %) y que todos los ISP más importantes son compatibles con ellas. Algunos cálculos dicen que es incluso mayor. Independientemente de la cifra exacta, la adopción de las DNSSEC en Suecia es impresionante en comparación con el resto del mundo, particularmente con Europa. ¿Cuáles fueron los pasos que dio Suecia para lograr esta alta adopción de las DNSSEC?

UW: The Swedish Internet Foundation lleva a cabo iniciativas para impulsar cambios. Nuestros registradores, que son también las empresas de alojamiento más importantes, obtienen una reducción del 5 % en los costos para los dominios firmados. No es un gran monto por dominio (aproximadamente € 0,60), pero si se firman 100.000 dominios, la cifra comienza a tener peso.

Además, tenemos una comunidad de ISP, empresas de alojamiento, registradores y entusiastas del DNS en la que se intercambia lo último sobre el DNS, pero donde también se intenta ayudar a los demás cuando algo sale mal.

GG: Los protocolos del DNS cifrado, como el DNS sobre HTTPS y el DNS sobre TLS, son cada vez más populares. Por supuesto, solo son compatibles con la autenticidad y la confidencialidad en vuelo, quizás de manera deliberada para lograr un diseño más modular. No obstante, esto no implica que no hagan nada para resolver el problema de que a menudo se usan registros DNS sin validar: los resolutores públicos que usen estos protocolos podrían, de todas formas, enviar registros sin firmar. ¿Cree que el desarrollo del DoT y el DoH son oportunidades que se perdieron para la promoción de las DNSSEC o piensa que es mejor que hayan apuntado a diferentes partes del rompecabezas?

UW: El DoH y el DoT tienen como objetivo principal la privacidad, mientras que las DNSSEC apuntan principalmente a la exactitud de los datos. Sin embargo, lo que me resulta raro es que las normas para los resolutores de confianza de los navegadores (p. ej., el programa de Mozilla) incluyan una larga lista de requisitos, pero las DNSSEC (la exactitud de los datos) no se encuentren entre ellos. Un resolutor de mi confianza debe ser compatible con ambos. Y esperamos que pronto también adopten el DNS del recursivo al autoritativo con cifrado.

GG: Recientemente, fue coautor de un *draft*, automatización de las DNSSEC (DNSSEC automation) y lo presentó en el Grupo de Trabajo de DNS Operations en la reunión IETF110. ¿Podría describir las motivaciones del *draft*?

UW: Como registro de .se, solo interoperamos con registradores, y no tenemos contacto directo con los registrantes. Si el registrador también es el operador del servidor de nombres, no suele haber problemas. Para un dominio, si el registrador no es el operador del servidor de nombres, los registrantes deben, de alguna manera, obtener los datos de las DNSSEC para su registrador. Y ahí está el problema. Además, aun si el registrador es el operador del servidor de nombres, el registrante tendrá que pasar por una serie de operaciones complejas si quiere cambiarse a otro registrador (o a otro operador de servidor de nombres), o arriesgarse a perder su seguridad (es decir, quedarse sin DNSSEC temporalmente).

Actualmente, en .se hemos decidido que queremos convertirnos en el primer ccTLD 100 % firmado. Uno de los desafíos es que cambiar el operador del servidor de nombres es realmente complejo. Así que, estábamos buscando una solución cuando llegaron Steve Crocker y Shumon Huque con su proyecto para automatizar las DNSSEC de múltiples firmantes. Resulta que cambiar el operador del servidor de nombres es un caso de uso especial de las DNSSEC de múltiples firmantes.

Lo que queremos hacer es describir los algoritmos sobre cómo iniciar y desplegar una configuración de múltiples firmantes y cómo implementar llaves o algoritmos. Los siguientes pasos serán crear una descripción sobre cómo hacerlo manualmente con el actual software del servidor de nombres, luego una descripción de la API que se necesitaría para la automatización, y finalmente la descripción de un protocolo para la automatización total del proceso para cambiar la información necesaria entre los servidores de nombres.

Con la ayuda de CDS/CDNSKEY y CSYNC, ya no es necesario que las comunicaciones se den fuera de banda. Específicamente, no es necesario que la información de las DNSSEC sea reenviada por el registrante.

GG: ¿Así que hay otros casos de uso de las configuraciones DNSSEC de múltiples firmantes?

UW: Por ejemplo, se necesitaría una configuración total de múltiples firmantes cuando se quieran usar grandes proveedores DNS diferentes. Supongamos que usted está administrando un numeroso grupo de máquinas que se encienden y se detienen todo el tiempo. Hace uso del DNS para llegar a esas máquinas y, por lo tanto, publica sus nombres en el DNS. Por seguridad operativa, usted no administra su propio DNS, sino que recurre a un importante proveedor de DNS, como Dyn o CIRA. Para una mayor tolerancia a las fallas, es probable que quiera usar ambos. Cada operador usará sus propias llaves para firmar y, por consiguiente, se necesita una configuración de múltiples firmantes.

Nuestro propio caso de uso —es decir, cambiar el operador del servidor de nombres— se puede considerar un caso de uso especial de la configuración.

Usted quiere cambiar los servidores de nombres y también quién controla las llaves DNSSEC del dominio. Ni el operador anterior ni el nuevo liberarán la llave privada. En ese caso, debemos unir a ambos operadores en una configuración de múltiples firmantes y, luego, el operador anterior debe salir de dicha configuración.

GG: Hacer la transición a una configuración de múltiples firmantes ciertamente es una manera excelente de cambiar los operadores de servidores de nombres. ¿Cómo fue su experiencia en la implementación de esto?

UW: De hecho, intentamos crear código ejecutable, pero resulta que los servidores de nombres actualmente no están equipados para gestionar esta configuración. Intentamos añadir registros DNSKEY adicionales a una zona con actualizaciones dinámicas, pero fracasamos estrepitosamente. Añadir llaves adicionales a través de una línea de comandos resultó ser toda una aventura. Tuvimos que usar nuestros contratos de soporte con proveedores para lograrlo.

Los CDS/CDNSKEY a menudo se automatizan, lo que implica que un servidor de nombres no publicará un registro CDS/CDNSKEY de una llave que no conoce. Sin embargo, esto es necesario en la configuración de múltiples firmantes.

Así que, actualmente, tenemos una versión relativamente testeada de los algoritmos necesarios. Nuestra colaboración con deSEC produjo una primera API funcional que permite publicar llaves adicionales, registros sincronizados de CDS/DNSKEY.

Pronto tendremos guías para las operaciones manuales de PowerDNS. Esperamos entablar una conversación con otros implementadores de software sobre esta compatibilidad.

GG: Ulrich, gracias por tan detallada explicación, por su tiempo, y por el increíble trabajo que hace en el IETF.

La espalda del camello: DNS del recursivo al autoritativo con cifrado

Por Gurshabad Grover

Con la proliferación del despliegue de los protocolos de transporte del DNS cifrado, como el DNS sobre HTTPS (DoH) y el DNS sobre TLS (DoT), podríamos llegar a pensar que la confidencialidad en vuelo de las consultas DNS es un problema del pasado. Un perfilamiento integral de las amenazas de seguridad, sin embargo, revela lo contrario.

En una charla durante el Taller de Privacidad del DNS del 2021, Daniel Kahn Gillmor asoció la Privacidad en el DNS a la armadura para un camello. El DoH y el

DoT brindan confidencialidad para las consultas DNS que van desde un usuario al resolutor recursivo, y solo cubren la mitad delantera del cuerpo del camello. Los resolutores recursivos, por otro lado, envían estas consultas a servidores autoritativos de una manera ampliamente desprotegida contra espectadores.

Los atacantes que monitorean el tráfico de texto plano entre un resolutor recursivo y un servidor autoritativo pueden, aun así, hacer inferencias sensibles sobre la actividad en línea de un usuario. Por ejemplo, quienes observan la ruta pueden correlacionar el momento de la consulta cifrada de un usuario (a un resolutor recursivo) con la consulta no cifrada consecutiva (del resolutor recursivo a un servidor autoritativo), y fácilmente sacar conclusiones sobre en qué sitios web navega el usuario.

Como mínimo, esta comunicación no cifrada ni autenticada permite que los atacantes intercepten o modifiquen las respuestas a las consultas y se hagan pasar por el servidor autoritativo. En palabras de Gillmor, es hora de que el IETF explore cómo hacer una armadura para "la parte trasera del camello".

(Resulta interesante que esta no es la primera vez que alguien compara al DNS con "un camello". En 2008, Bert Hubert condenó la creciente complejidad de los registros DNS y expresó preocupaciones acerca de agregar otra función al DNS, diciendo que sería lo que le rompería la espalda al camello. Anteriormente, en el 2000, Randy Bush planteó problemas similares y preguntó si el IETF no estaba "sobrecargando la espalda de un caballo viejo". Al observar este cambio gradual en la metáfora, podríamos tentarnos a concluir que un camello es un caballo diseñado por un grupo de trabajo del IETF).

Si bien ha habido conversaciones acerca de cifrar las consultas DNS del recursivo al autoritativo desde 2019, el Grupo de Trabajo (WG) de DNS Privacy Exchange (DPRIVE) adoptó una propuesta concreta recién en febrero del 2021. En la reunión del grupo de trabajo en la IETF110, Peter van Dijk presentó esta propuesta, DNS del recursivo al autoritativo con cifrado (Recursive to Authoritative DNS with Encryption), que describe una manera de que los resolutores recursivos descubran si los servidores autoritativos son compatibles con el DNS cifrado. Esto se logra simplemente comprobando la existencia de un registro TLSA del DNS en un servidor autoritativo, que especifica las llaves que se usarán para el servidor TLS de ese dominio.

El *draft* expone un protocolo que es compatible con dos casos de uso. El primer caso, el cifrado completamente autenticado, es para resolutores recursivos que solo quieren enviar consultas cifradas y, por lo tanto, fallan si no logran contactar un servidor autoritativo usando una conexión cifrada. El segundo caso de uso está basado en el principio de seguridad oportunista; es decir, se prefiere un nivel de protección relativo incluso si la protección total no está disponible o no es posible en todo momento. En este caso, los resolutores recursivos son compatibles con

consultas cifradas a los servidores autoritativos, pero puede que no siempre sea la opción predeterminada o no siempre la apliquen.

Es probable que un factor clave que puede influenciar el despliegue de la propuesta sea el nivel de control que se les permite a los servidores autoritativos en cuanto a cómo señalan la compatibilidad con el cifrado.

La propuesta ya está enfrentándose a rechazos por parte de los operadores de servidores raíz. En una declaración emitida el 30 de marzo, cuestionaron los beneficios de cifrar consultas dirigidas a los servidores de nombres raíz. Es entendible, dado que el riesgo de privacidad de una consulta expuesta dirigida a un servidor raíz es mucho menor que aquel de una consulta que se dirige a un servidor autoritativo para dominios de segundo nivel.

La declaración también menciona que pasar de protocolos sin estado y sin cifrado (UDP) a protocolos cifrados basados en la conexión (como TLS) creará un rendimiento no deseado en general. También argumentan que los costos adicionales de red y computación harán que los servidores sean más vulnerables a los ataques de denegación de servicios.

Como comentario sobre esta declaración, Daniel Kahn Gillmor le dijo a CENTR: “Si bien es decepcionante que los operadores de servidores raíz no tengan la capacidad técnica para desplegar ninguno de los mecanismos de DNS cifrado estandarizados en el futuro próximo, me dio gusto ver que apoyaran fuertemente la minimización de QNAME y el cacheo agresivo de las DNSSEC, que brindan beneficios de privacidad significativos tanto para los usuarios como para los dominios”.

Gillmor agregó que “parece apropiado que los operadores de servidores raíz estén dispuestos a seguir el liderazgo de otros segmentos de la jerarquía del DNS en el despliegue del DNS autoritativo cifrado”.

Más abajo en la jerarquía, entre los servidores autoritativos para los dominios de segundo nivel, aún parece no haber un claro consenso sobre la viabilidad de la propuesta. En los próximos meses sabremos si las preocupaciones sobre el rendimiento prevalecerán ante la necesidad de mayor seguridad y privacidad. Porque, a veces, es más fácil que un camello pase por el ojo de una aguja que esperar que una mejor solución de seguridad logre un despliegue popular.