Informe de CENTR

IETF 104

Praga, 22-29 de marzo de 2019

Traducción - LACTLD

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

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

LACTLD
Latin American and Caribbean ccTLDs Organization

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

Contenidos

Aspectos destacados **3**

Debates sobre el DoH 3

¿Listas exhaustivas? 3

Bandos enfrentados: el bando de la red vs el bando de los navegadores – comunidad DNS dividida 5

Mozilla anuncia los próximos pasos para el DoH 6

Descubrimiento DoH 7

Debate sobre el DoH: ¿qué sigue? 8

Operar el DNS de una manera más amigable con la privacidad: ¿un servicio especial o para todo el DNS? 9

Repercusiones de los ataques DNSPionage: el debate sobre la estandarización del bloqueo ("lock") de registro 12

DNSpionage: ataques dirigidos a la infraestructura del DNS como abrepuertas a víctimas 13

Bloqueo de seguridad/registro 13

Conclusión de una víctima de DNSpionage 14

Grupos de Trabajo y reuniones BoF **16**

WG de DPRIVE: el camino del recursivo al autoritativo sigue siendo un tema 16

¿Los usuarios señalan sus deseos de privacidad? 16

Más soluciones alternativas para la privacidad del DNS 17

El RDAP en regext IETF: ¿relacionado con la privacidad/las políticas o no? 17

Todo RDAP, y algunas preguntas de políticas 18

DNSOP – DNSSEC: las cookies del servidor DNS y la "organización" del lío de los TLD especiales 19

RG de SMART: los "datos cifrados" se quitaron de la lista de objetivos 20

Seguridad incompatible con la resiliencia 20

Primer documento draft en SMART 21

La BoF más rara: logos de marcas validadas en e-mail 21

Noticias del IETF **23**

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

Aspectos destacados

Debates sobre el DoH

La implementación de DNS sobre HTTPS (DoH) por parte de Mozilla y Google, quienes recientemente hicieron anuncios sobre su uso del DoH en sus respectivos navegadores, avivó los debates existentes sobre el DoH durante la semana del IETF 104. Tanto el Grupo de Trabajo de DPRIVE como el de DoH debatieron el DNS sobre HTTPS (RFC8484). La reunión del WG de DoH tuvo la intención de centrarse en el futuro descubrimiento de servidores DoH. La reunión del WG de DPRIVE dedicó tiempo a que Vittorio Bertola de Open-Xchange presentara un draft sobre pautas de implementación posibles para clientes DoH. La propuesta de Bertola se asemeja, en cierto modo, al trabajo actual de Sara Dickinson para una BCP sobre implementaciones de privacidad para los servidores DNS, que, en un principio, comenzó teniendo en mente el DNS sobre TLS. Además de estas reuniones, una reunión paralela especial organizada por Stéphane Bortzmeyer (Afnic) les brindó a los dos (¿o tres?) bandos más tiempo para desahogarse sobre lo que algunos operadores de red y de DNS consideran como un golpe de estado contra sus modelos de negocios.

¿Listas exhaustivas?

A esta altura, los operadores de red ya se han dado cuenta del posible cambio masivo que podría causar el DoH al absorber las consultas DNS de sus clientes. En lugar de que el resolutor DNS esté controlado por el correspondiente operador de red, las consultas DNS enviadas a través de navegadores las responderán resolutores externos. Hasta ahora, estos resolutores fueron elegidos por las compañías de navegadores. La red mundial de resolutores de Cloudflare es, actualmente, el único operador DoH contratado por Mozilla y Google. Para el navegador de Chrome, las consultas serán resueltas mediante la propia red de resolutores de Google. Mientras no exista un mecanismo de descubrimiento más amplio para diferentes servidores DoH, el cambio de DNS a DoH tendrá como consecuencia una concentración importante de tráfico DNS.

La concentración del mercado se ha ubicado, por lo tanto, como una de las preocupaciones principales en dos documentos de la autoría/coautoría de operadores de telecomunicaciones importantes que están interviniendo en el debate sobre el DoH. Comcast y British Telecom se asociaron con Sky y el Instituto de Tecnología de Georgia para escribir el documento “Centralized DNS over HTTPS (DoH) Implementation Issues and Risks” (DNS sobre HTTPS [DoH] centralizado: problemas y riesgos de implementación) y con Deutsche Telekom, Open-Xchange y el reconocido experto en DNS Jim Reid para escribir “DNS over HTTPS (DoH) Considerations for Operator Networks” (DNS sobre HTTPS [DoH] Consideraciones para los operadores de red).

En el documento de descentralización, los operadores expresan estar sorprendidos por la forma de activación de DoH en las implementaciones de navegador: “Parece no tener precedentes que un protocolo nuevo pueda ser desplegado tan rápidamente y, así, desplazar un protocolo existente, duradero y ampliamente distribuido”. También enumeran problemas en relación con la posible centralización del tráfico DNS:

- *cambio del ecosistema de Internet por el desplazo del tráfico a unas pocas plataformas*

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

- *menor estabilidad a través de menos puntos de fallo (reconociendo que la concentración del tráfico DNS no es nueva)*
- *posibles problemas de seguridad a través de menos puntos de fallo, permitiendo que el atacante vaya por apenas unos pocos sitios (incluso ataques dirigidos a administradores DNS individuales)*
- *pérdida de una visibilidad más amplia de amenazas para la seguridad*
- *pérdida de control parental y otros tipos de control de contenidos*
- *problemas para el DNS dividido ("split DNS") y posibles filtraciones de dominios de uso interno mediante solicitudes DoH*
- *reducción de la diversidad de software debido a menor cantidad de actores*
- *más uso comercial de los datos del DNS*
- *posibles problemas para la localización (la "razón de ser" para la gestión del tráfico de redes de distribución de contenido (CDN), posibles efectos de latencia)*
- *DoH como fuente de malware o comando y control (HTTPS://github.com/SpiderLabs/DoHC2/blob/master/Mitre_Attackcon_Playing_Devils_Advocate_With_Attack_1.0.pdf)*
- *problemas con el bloqueo de DNS exigido por ley (y alteración de "jardines vallados" o portales cautivos)*
- *mayor complejidad, dificultades con la resolución de problemas debido a los proveedores adicionales desconocidos por los usuarios finales*
- *riesgos de negocios planteados por la concentración (mercado de software DNS más pequeño, menos opciones de operadores de DNS públicos, mercado más pequeño para las CDN, mercado laboral DNS más pequeño)*

El documento de centralización también brinda varias recomendaciones, que incluyen exigir la estandarización del descubrimiento DoH, y la necesidad de que los operadores DNS convencionales empiecen a probar el DoH y, a la vez, ralentizar la implementación a través de navegadores mediante una combinación de pasos técnicos y políticos/administrativos. Esto implica: más tests y medidas; no permitir que el DoH sea el valor por defecto; una revisión de ICANN; evaluación comunitaria; pedir la implementación de DNSSEC; la elaboración de pautas de privacidad de datos para el DoH centralizado.

Si bien el documento sobre consideraciones enumera la mayoría de los problemas anteriores, también aborda los cambios que resultan del DoH desde una perspectiva operativa. Esto incluye aspectos como posibles problemas con traducción de direcciones de red (NAT) IPv6-IPv4, fallas en recuperación/informes de falla/asistencia al usuario, y la cuestión del "consentimiento informado" de los usuarios. Con el DoH, la prestación de DNS y la conectividad a Internet pueden ser desvinculadas, y puede que los usuarios, sin saberlo, se conviertan en clientes de partes a las que no conocen. Para diferentes aplicaciones, en un futuro, es posible que el DNS sea provisto por diferentes partes y mediante diferentes protocolos.

Una pregunta básica según los proveedores de red es: ¿quién decidirá qué servidores DNS (y qué protocolos) se usarán en el futuro: los proveedores de conectividad, los proveedores de navegadores/aplicaciones, los usuarios?

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

Bandos enfrentados: el bando de la red vs el bando de los navegadores – comunidad DNS dividida

Hubo una reacción bastante negativa ante las presentaciones de los proveedores de red (Jason Livingood, Comcast, hizo una presentación durante la sesión del DoH, y Jim Reid durante la sesión dedicada a la concentración). En definitiva, se formaron tres bandos en las discusiones sobre el DoH. Se pueden describir como: el bando de navegadores/HTTPS/web (con Mozilla y su proveedor Cloudflare y Google a la cabeza) y, el bando opuesto, proveedores de conectividad/red (grandes telcos que ya temen perder contra el consorcio Google/Amazon/Facebook/Apple). El tercero está compuesto por aquellos proveedores DNS que buscan usar DoH lo mejor que puedan.

La comunidad DNS parece estar dividida. Varios operadores DNS (por ejemplo, PowerDNS), y varias CDN como Akamai (Ralf Weber planteó su caso en Praga) rechazan el cambio hacia una cantidad pequeña de resolutores de confianza fuera de sus redes de servicio. Sin embargo, también hay operadores DNS que se enfocan en los posibles efectos positivos con respecto a la privacidad y a los efectos antifiltraciones. Ellos recomiendan reconsiderar la implementación de una manera más descentralizada. Los representantes de Afnic y CZ.NIC hicieron comentarios respecto a esto.

Los defensores de la privacidad que trabajan en organizaciones de la sociedad civil y los desarrolladores de software DNS de código abierto cuestionan los argumentos de las telcos en contra del DoH. Señalan las similitudes con intentos anteriores de rechazos de las telcos en contra de un mejor cifrado del tráfico (por ejemplo, en QUIC y TLS 1.3). Junto con los expertos en DNS y el grupo de navegadores, hacen referencia a una lista de preocupaciones demasiado larga en los drafts.

Daniel Kahn Gillmor, un experto técnico de la Unión Americana de Libertades Civiles (ACLU) expresó claramente que el pedido de las telcos sobre el consentimiento informado llega demasiado tarde: “El DoH nos obligó a luchar con la idea de que estamos filtrando datos. Jamás les habíamos informado a los usuarios. Ahora podemos cambiar a quién llegan estos datos, y esto pone mal a ciertas personal”. Con muchos usuarios (en EE. UU.) que no pueden elegir cuando se trata de proveedores de conectividad, y sin tener una legislación vigente similar al GDPR, la resolución actual del DNS como valor predeterminado “no es necesariamente más respetuosa con la elección del usuario”. Aun así, el activista señaló que sí estaba “de acuerdo con aquellos que están aterrados por el DNS sobre Cloudflare. Pero eso no es un problema del DoH”.

El director de tecnología (CTO) de Mozilla, Eric Rescorla, quien prominentemente lideró el debate a favor del DoH en Praga, también reforzó el argumento que expone a los operadores de red que pueden y, casi siempre, interfieren con los atacantes de la resolución del DNS: “Alguien que controla la red, pero no tu computadora, es un atacante”. Rescorla sí reconoció la necesidad de “asegurarse de que el nivel de la web no esté filtrando información”, ya que “con la multiplexación, es posible la filtración”. Sin embargo, pidió centrarse más en los aspectos positivos del DoH y en los motivos técnicos y las políticas que aseguran la protección contra la posible filtración de datos. Rescorla señaló que, si bien el GDPR se mencionó mucho en el debate como una política que protege a los usuarios contra la filtración de datos de los servicios DNS (en la UE), no aborda la filtración y el bloqueo por parte de proveedores DNS locales.

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

De estos debates, se pone en evidencia una diferencia fundamental: las telcos intentan abogar por el "buen bloqueo" (control parental, filtrado de malware por parte del proveedor de red, bloqueo de sitios que se consideran ilegales en una determinada jurisdicción) y proponen la idea de que el cifrado del DoH podría ser necesario solo para "disidentes" (en países sin rule of law). Sin embargo, la comunidad de navegadores piensa a la interferencia por parte de un proveedor de red ("alguien con control total o parcial de la red", según Rescorla) como una suerte de "ataque" en cualquier lugar del mundo.

Mozilla anuncia los próximos pasos para el DoH

Durante la semana del IETF, Rescorla anunció los próximos pasos (sin un cronograma claro) en relación con la estrategia del DoH, y, en este anuncio, reconoció las preocupaciones relativas a la concentración. Rescorla reiteró que había "mucha evidencia del monitoreo/manipulación del tráfico de los usuarios mediante este vector".

Según su CTO, a Mozilla "le gustaría desplegar el DoH como valor predeterminado para nuestros usuarios" y "seleccionar un conjunto de resolutores recursivos de confianza (TRR) que usaremos para la resolución del DoH". Para lidiar con los problemas de privacidad, los futuros TRR deberían adherirse a las políticas de privacidad establecidas por Mozilla que "coincidirían grosso modo" con las que creó Mozilla para los resolutores de Cloudflare que se usan actualmente.

Las políticas de privacidad tendrían que refinarse, según la declaración, pero estarían basadas en los siguientes puntos:

1. Las copias de Firefox se configurarán con un conjunto de TRR. Diferentes regiones pueden tener diferentes conjuntos de TRR o diferentes valores predeterminados. Además, podemos tener DoH/TRR como valor predeterminado en algunas regiones y no en otras, especialmente al comienzo.
2. A los usuarios se les informará que hemos habilitado el uso de un TRR y es posible apagarlo en ese momento, pero no se requerirá aceptar previamente para obtener DoH con un TRR.
3. Cualquier cliente seleccionará automáticamente un resolutor de ese conjunto y usará ese para todas las resoluciones [con las dos excepciones que se mencionan más abajo*].
4. En cualquier momento, el usuario tendrá la posibilidad de seleccionar un resolutor diferente de la lista, especificar su propio resolutor, o inhabilitar el DoH por completo.

*Las excepciones son: los casos en los que la red también controla al cliente (por ejemplo, son capaces de administrarlo de manera remota mediante MDM); en este caso, el correspondiente usuario/red debería ser capaz de seleccionar un resolutor y/o inhabilitar el DoH. También, cuando un sistema tiene un resolutor preferido que está en la lista de TRR de Mozilla, debería ser posible elegir (quizás, escribió Rescorla, a través del draft de descubrimiento de DoH de Paul Hoffman).

A corto plazo, la necesidad de que los resolutores estén en la lista de Mozilla "plantea algunos desafíos para los operadores de resolutores. Estaríamos dispuestos a debatir cómo adaptar nuestras restricciones de seguridad para satisfacer las necesidades de múltiples aplicaciones,

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

para que, a medida que más sistemas desplieguen el DoH/TRR, puedan compartir una lista de resolutores aprobados por un estándar en común".

Con solo permitir que los operadores de red (o los usuarios, que, según Rescorla, no deberían tener que decidir sobre sus resolutores) "dicten el resolutor DoH, se obviaría el objetivo de seguridad" previsto.

Mientras tanto, Mozilla publicó las políticas de privacidad (incluidas las políticas de transparencia) que enumeran: una limitación para retener datos (24 horas solamente, siempre y cuando los datos no estén anonimizados); una prohibición para comercializar/vender/transferir los datos (excepto las transferencias exigidas por ley); una prohibición para combinar/agregar esos datos con datos de otras fuentes; y una prohibición para vender/conceder acceso a ellos. Curiosamente, Mozilla obliga a los candidatos TRR a soportar minimización de consultas, pero no a implementar DNSSEC. Si bien la compañía recibiría muy bien la validación de DNSSEC por parte del resolutor DoH, pensaron que no debería ser obligatoria, según escribieron los representantes de la empresa en un debate en la lista de correos.

Se puede ver una lista de servidores, navegadores y herramientas DoH aquí.

Descubrimiento DoH

Todos los "bandos" concuerdan, en esencia, en un punto. Es necesario establecer un mecanismo para permitir la elección del resolutor. Varios oradores en la reunión sobre el DoH en Praga hicieron referencia a esto en los anuncios de Mozilla sobre los próximos pasos, remarcando que era indispensable para luchar contra una mayor consolidación o concentración del mercado en el mercado DNS. "Sin un mecanismo de descubrimiento, no tendríamos más opción que Cloudflare y Mozilla", dijo Petr Spacek, de CZ.NIC, durante el debate. El WG de DoH debatió el correspondiente draft de descubrimiento editado por Paul Hoffman, de ICANN.

En resumen, el draft reconoce que es probable que los clientes quieran usar un servidor interno o uno externo preferido para la resolución del DNS. Por lo tanto, el draft propone "protocolos para obtener la lista de plantillas URI [RFC6570] o direcciones para los servidores DoH asociados con al menos uno de los resolutores que esté usando el sistema operativo sobre el que funcione la aplicación". Los dos mecanismos contemplados son "servidores DoH de HTTPS" para usar "una URI conocida [I-D.nottingham-rfc5785bis] que se pueda resolver para devolver las plantillas URI en una respuesta HTTP" y "servidores DoH de DNS" que pongan direcciones de resolutores en un nuevo nombre de dominio de uso especial (SUDN) [RFC6761] "que puedan consultarse para que devuelvan las plantillas URI como TXT Rrset" (o permitir consultar a los resolutores de un SUDN para Rrsets A y AAAA). Los navegadores deben tener una entrada especial en su interfaz de configuración en la que los servidores DoH permitidos para los servidores DNS tradicionales (Do53) o DNS sobre TLS (DoT) se puedan ver ("servidor DoH asociado con mi resolutor actual"). Ted Hardie (presidente de la IAB) presentó algunos de los pensamientos preliminares sobre el problema de la naturaleza de los nombres de dominio especiales y su relación con la raíz de ICANN.

No obstante, uno de los principales temas de controversia tuvo que ver con asegurar que, al elegir los resolutores, los clientes (usuarios finales) no sean descarriados y llevados a las manos de actores maliciosos que, entonces, ni siquiera tendrían que realizar un envenenamiento de

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

caché u otros reenrutamientos del DNS para “adueñarse” de los usuarios finales en cuanto a su consulta DNS y la capacidad de vender una visión del DNS imparcial o incluso falsa.

Estos problemas de seguridad se mencionan claramente en el draft (junto con los posibles problemas de privacidad causados por TLS como HTTPS, que permiten la “identificación de usuario de maneras que el simple Do53 no admite”):

“Si las consultas DNS enviadas desde resolutores stub a resolutores recursivos no se envían mediante transportes que garanticen la integridad de los datos y la autenticación del servidor, los protocolos ‘servidores DoH de DNS’ y ‘direcciones de resolutor de DNS’ quedan expuestos a atacantes en el camino que dirigen a un usuario a un servidor DoH que, en realidad, no está asociado con su resolutor. El Do53 no es un transporte seguro; pero tampoco lo es el DoT con el perfil oportunista”.

Tanto Rescorla como Patrick McManus de Mozilla dijeron que era imposible autenticar fuentes no autenticadas. Esto explica la reticencia de Mozilla a abrir demasiado la elección de resolutor, incluida, quizás, la idea de la elección por parte del usuario final.

En el WG de DPRIVE, se presentó un draft sobre cómo organizar el descubrimiento del servidor DoH (y DoT) manteniendo intactos el “DNS dividido” (split DNS) o el monitoreo de seguridad del proveedor. El concepto, en la práctica, busca usar un servidor de “Registro de Transporte Seguro” (EST) en la red del proveedor como un punto de control para el descubrimiento DoH y DoT para el cliente (usuario final). Esto habilitaría al proveedor a permitir un transporte seguro (sin bloquear DoT ni DoH) y, al mismo tiempo, dejar que continúen con el monitoreo de seguridad, explicó Tiru Reddy (McAffee), durante el WG de DPRIVE. Al insertar este punto de control en el borde de la red, el “DNS dividido” sería posible nuevamente.

Debate sobre el DoH: ¿qué sigue?

Se dejó en claro otro punto en los intentos de llegar a una “tregua” entre los varios grupos del DoH: en específico, que los debates no deberían cuestionar el protocolo de DNS sobre HTTPS (RFC8484). En cambio, el foco debería estar en cómo se implementará el DoH. Por lo tanto, el draft sobre descubrimiento DoH debería recibir especial atención. Abordar las preocupaciones sobre la implementación y el funcionamiento también es el tema de dos drafts que se están debatiendo actualmente en el WG de DPRIVE (ver a continuación).

Otra idea que se planteó, mientras tanto, en la lista de correos del DoH es la de un puerto especial para el DoH. Para facilitar la configuración del DoH como valor predeterminado, según Tomas Krizek, de CZ.NIC, se prevé “usar (el puerto) 44353 como el puerto por defecto para el DoH” para Knot Resolver. Krizek escribió que usar el puerto clásico HTTPS 443 para el DoH causaba conflictos. Hubo mucha oposición contra esta idea: algunos se quejaban de que usar un nuevo puerto complicaría la implementación del DoH, pero también de que la mera idea de esconder el tráfico DNS dentro del tráfico HTTPS quedaría destruida con un puerto especial —que sobresaldría como el puerto DoT 853. Los desarrolladores de CZ.NIC, por otro lado, expresan que no esperan llegar a un rápido consenso sobre el draft del descubrimiento y consideran que la solución de un puerto extra es una manera de facilitar el despliegue.

Lo que complica el debate sobre el DoH está repartido en varios factores. El WG de DoH, luego de aprobar el estándar DoH básico, está trabajando en el descubrimiento DoH. Los problemas operativos y los documentos de BCP para los implementadores están actualmente cubiertos en

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

el WG de DPRIVE. Ninguno de estos grupos está interesado en encargarse de los nuevos drafts centrados en los problemas operativos y de concentración. Y, en el WG de DNSOP, la copresidenta Suzanne Woolf se apresuró para remarcar que estos no eran problemas para el DNSOP.

McManus piensa que, en un futuro, se puede revivir el trabajo relacionado con posibles mecanismos para incluir respuestas DNS adicionales al responder consultas al cliente. Dicho trabajo posiblemente sería para el HTTPBis.

Para complicar aún más el debate, el IESG consideró necesario crear otra nueva lista de correos (el DoH ya se debate en las listas de correo de DoH y de DPRIVE, como mínimo). La lista de correos de aplicaciones Applications Doing DNS (ADD), según el nuevo director de área (ART), Barry Leiba, estará dedicada a "DNS sobre HTTPS, DNS sobre TLS, sus opciones de implementación, uso de aplicaciones, preocupaciones operativas, preocupaciones de privacidad, preocupaciones de desempeño, y cualquier otra del estilo". Leiba alentó a los ingenieros a "llevar todo el debate relacionado a la nueva lista y abstenerse de discutirlo en DoH, DPRIVE, DNSOP, y cualquier otra lista". Si bien Leiba dijo que la motivación de ADD, que también se puede convertir en un WG, era "evitar la fragmentación", por ahora, solo parece propiciar la fragmentación, especialmente dado que, según reconoció Barry Leiba, partes del trabajo ciertamente entraban en el alcance de otros WG.

Leiba previó una posible BoF en Montreal (IETF 105) "destinada a formar un grupo de trabajo de 'ADD', probablemente en el Área ART, pero con una fuerte interdisciplinariedad esperada y bienvenida por parte de OPS, SEC, INT, y probablemente del resto del sistema solar de la comunidad del IETF".

El debate sobre DoH-DoT, según algunos observadores, podría ser mayor, y debería, en lo posible, estar guiado por toda la comunidad IETF. Durante la reunión paralela especial para el DoH, un participante mencionó la idea de formar un WG de Derechos Humanos/Privacidad. Sara Dickinson (Sinedun), quien el año pasado instó a la comunidad DNS a analizar exhaustivamente los cambios que podría traer el DNS sobre HTTPS, pidió, durante el WG de DPRIVE, que se considere un posible nuevo WG que se dedicara de manera más general a las cuestiones de políticas y despliegue.

Actualmente, Dickinson es copresidenta del Grupo de Investigación de Evaluaciones y Mejoras de Privacidad (en el IRTF) recientemente establecido y está editando una versión bis del documento sobre Consideraciones de Privacidad del DNS (RFC7626) y un documento de Mejor Práctica Actual (BCP) para operadores de servicios de privacidad del DNS.

Operar el DNS de una manera más amigable con la privacidad: ¿un servicio especial o para todo el DNS?

Durante la sesión de DPRIVE en Praga, Dickinson presentó ambos documentos: la versión bis de las Consideraciones de Privacidad y el documento de Mejor Práctica Actual "Recomendaciones para los Operadores de Servicios de Privacidad del DNS". El documento de seguimiento (bis) sobre la RFC de consideraciones de privacidad se había convertido en una necesidad, dados los significativos cambios de los últimos tres años. La adopción de las dos RFC de DoH y de DoT marcó pasos importantes para los operadores de servicio DNS. Además de considerar nuevas amenazas —por ejemplo, las amenazas que heredan los servicios DNS de

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

tomar transporte HTTPS (riesgo de rastreo) y los ataques al transporte cifrado—, el documento también incluye secciones sobre el bloqueo de servicios cifrados y sobre problemas existentes sobre datos personalmente identificables en el “payload” del DNS (Cookies DNS, ECS).

La BCP se asemeja al documento sobre las preocupaciones de privacidad, ya que brinda una serie de estándares mínimos (y recomendaciones u optimizaciones) que los operadores deberían cumplir si quieren que su servicio sea un servicio de privacidad del DNS. El documento aborda las mejores prácticas para los datos en el cable (del resolutor stub al recursivo), los datos en reposo (minimización de datos) y el tráfico ascendente. También incluye un capítulo especial sobre una “declaración de políticas de privacidad y prácticas del DNS”. Dicha declaración, si se la estandariza, permitiría a los usuarios (y a las partes que monitorean) comparar diferentes opciones que puedan tener de distintos operadores. Las políticas que se deben cubrir son el manejo y potencial registro de las direcciones IP (¿”Información de Identificación Personal” o no?), la naturaleza y condición (¿anonimización?) de la agregación y transferencia de datos, los tiempos de retención de datos, las políticas de compartición o venta de datos, la declaración de socios informados, las prácticas de correlación de datos, las políticas de filtrado (¿legales u otros filtrados constantes?). Una declaración de prácticas debería exponer las prácticas operativas actuales y sus desviaciones, la jurisdicción, los acuerdos con agencias de aplicación de la ley, los mecanismos para que los usuarios se pongan en contacto con el operador, y debería hacer cumplir estas políticas y las de consentimiento del usuario.

Dickinson y el proyecto de DNSprivacy crearon tablas que ilustran cómo sería una comparación entre políticas relevantes y prácticas reales. Dickinson señaló que debió leer 7000 líneas de letra chica para poder elaborar estas tablas. Una DPPPS estandarizada permitiría una comparación y un monitoreo más sencillos. Hubo un breve debate en el WG de DPRIVE sobre la posibilidad de que el marco de la DPPPS se vuelque en un documento especial, y algunos participantes (como Dan York, de ISOC) estuvieron a favor de esto, ya que los destinatarios serían diferentes para los documentos de los operadores y de la declaración de políticas de privacidad.

Rich Salz (Akamai) solicitó incluir recomendaciones con respecto a cómo deberían funcionar las CDN con los servicios DNS con mejoras de privacidad.

Con respecto a las Mejores Prácticas Actuales, el WG también habló sobre la posibilidad de añadir otro documento de recomendaciones de BCP que se centre en los clientes (en lugar de los servidores). Dickinson afirmó que quizás era un buen momento para añadir esta BCP con recomendaciones de privacidad del DNS del lado del cliente. Indicó que sería posible incorporar las recomendaciones de su draft dirigidas a los clientes en un documento nuevo, aunque se superpondría en parte con un draft presentado por Vittorio Bertola (OpenX-Change) durante el WG de DPRIVE. Las “Recomendaciones para Aplicaciones de Privacidad del DNS del lado del Cliente” de Bertola se elaboraron como contribución al debate sobre el DoH, pero fueron mejor recibidas que los documentos de Telcos/ISP.

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

Policy

List Item	1	2	3				4		5	6	7	
Redirect NXDOMAIN	IP address are PII	IP address logging	Clear list of what data stored and for how long	Share anonymized data with partners	Share identifiable data with partners	Share or sell data to third parties	Exceptions to collection for attack analysis	non-profit	Partners	Combine DNS data with other data sources	Redirect NXDOMAIN	Block domains
Quad9 Secure	Y	N	Y	Y	N	N	Y	Y	IBM PCH GCA	N	N	Y
Quad9 Unsecured	Y	N	Y	Y	N	N	Y	Y		N	N	N
Cloudflare	Y	N	Y	Y	N	N	N	N	APNIC	N	N	?
Cloudflare DoH	Y	N	Y	Y	N	N	N	N	Mozilla/ Firefox	N	N	?
Google	N	Y(1)	Y	?	?	?	N	N	?	N	N	N(1)
OpenDNS	Y	Y	N	?	Y	Y	?	N	?	Y	N	?

(1) Only in temporary logs

Configuration Matrix		TLS	TLS 443	Strict Name	Strict SPKI	Cert 0	Cert 14	QNAME min	RTT 250	DNSSEC	Keepalive	Padding	TLS 1.3	OOOR
dnsovertls.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
dnsovertls1.sinodun.com	v4	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
	v6	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	!	✓
getdnsapi.net	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dns.quad9.net	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	!
dns.google	v4	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
	v6	✓	!	✓	●	✓	✓	!	✓	✓	!	!	✓	✓
1dot1dot1dot1.cloudflare-dns.com	v4	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
	v6	✓	!	✓	●	✓	✓	✓	✓	✓	!	✓	✓	✓
security-filter-dns.cleanbrowsing.org	v4	✓	!	✓	●	✓	✓	!	!	✓	!	!	!	!
	v6	●	●	●	●	●	●	●	●	●	●	●	●	●
unicast.censurfridns.dk	v4	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
	v6	✓	!	✓	✓	✓	✓	!	✓	✓	!	!	!	✓
kaitain.restena.lu	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
	v6	✓	!	✓	✓	✓	✓	✓	✓	✓	!	!	!	!
dnsovertls3.sinodun.com	v4	✓	!	!	✓	!	!	!	✓	✓	✓	✓	✓	✓
	v6	!	!	!	!	!	!	!	!	!	!	!	!	!
dnsovertls2.sinodun.com	v4	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	!

Bertola subrayó que el objetivo del documento no era detener el DoH, sino esclarecer problemas y posibles mitigaciones desde el punto de vista del cliente/aplicación. Durante la reunión de DPRIVE, Bertola aclaró los dos conceptos básicos posibles; el actual, donde los resolutores DNS son elegidos por defecto por la red donde se encuentra el usuario (aunque mantiene la opción de

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

configurar otros servidores DNS) y uno posible en el futuro, en el que las aplicaciones vienen con su propia opción de resolutor (de confianza) DNS.

Network-level	Application-level
All applications use the same resolver (the operating system one)	Each application uses its own resolver
The default is usually the resolver automatically suggested by the network	The default is usually supplied by the application (no local resolver discovery)
The user is in charge, either accepting the default or changing it in a single place	The application is at least partly in charge, choosing the default and/or constraining the choice to its own «trusted resolvers»

Los problemas que deben abordar los clientes DoH, según Bertola, son:

1. *Modelo de confianza y elección del usuario*
2. *Consolidación*
3. *Fragmentación de espacio de nombres*
4. *Privacidad*
5. *Control de acceso a contenido*
6. *Gestión de red y seguridad*
7. *Jurisdicción*
8. *Recuperación ante desastres*
9. *Asistencia al usuario*

Con el debate sobre el DoH apenas armándose, parece que habrá una lucha importante en la comunidad DNS. Varios operadores DNS ya han anunciado que también intervendrán en el DoH. Para que el DNS se mantenga “un poco” descentralizado (o que se acerque más a la descentralización), es necesario invertir tiempo, energía y fondos en la evolución del DNS.

Repercusiones de los ataques DNSPionage: el debate sobre la estandarización del bloqueo (“lock”) de registro

Los recientes ataques DNSpionage dirigidos a varias autoridades públicas de países del Medio Oriente (en particular, Líbano, Irak y Egipto) provocaron debates intensos sobre más mecanismos de seguridad para las registraciones de dominios. Alex Mayrhofer organizó una reunión paralela especial para evaluar la posibilidad de usar un bloqueo de registro estandarizado como contramedida. Si bien muchos registros ofrecen algún tipo de bloqueo, los participantes de la reunión en Praga advirtieron que el bloqueo en sí mismo se podría “convertir en un arma”. Después de cambiar el servidor de un nombre comprometido, el atacante podría pedir el bloqueo, complicando así las contramedidas del dueño legítimo.

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

Servidores atacados según Brian Krebs

nsa.gov.iq: el Consejo de Seguridad Nacional de Irak
webmail.mofa.gov.ae: e-mail del Ministerio de Relaciones Exteriores de Emiratos Árabes
shish.gov.al: el Servicio de Inteligencia Estatal de Albania
mail.mfa.gov.eg: servidor de mail del Ministerio de Relaciones Exteriores de Egipto
mod.gov.eg: Ministerio de Defensa de Egipto
embassy.ly: Embajada de Libia
owa.e-albania.al: el portal de acceso web de Outlook del portal electrónico del gobierno de Albania
mail.dgca.gov.kw: servidor de e-mail de la Dirección General de Aviación Civil de Kuwait
gid.gov.jo: Dirección General de Inteligencia de Jordania
adpvpn.adpolice.gov.ae: servicio de VPN de la Policía de Abu Dhabi
mail.asp.gov.al: e-mail de la Policía Estatal de Albania
owa.gov.cy: acceso web a Microsoft Outlook del gobierno de Chipre
webmail.finance.gov.lb: e-mail del Ministerio de Finanzas del Líbano
mail.petroleum.gov.eg: Ministerio de Petróleo de Egipto
mail.cyta.com.cy: telecomunicaciones y proveedor de Internet Cyta, Chipre
mail.mea.com.lb: acceso a e-mail de Middle East Airlines

DNSpionage: ataques dirigidos a la infraestructura del DNS como abrepuertas a víctimas

Los ataques DNSpionage combinaron varios vectores de ataque conocidos para lograr lo que los expertos llamaron un tipo de ataque completamente nuevo. Según Patrick Fältström (Frobbit), los atacantes utilizaron credenciales robadas, por ejemplo, para cambiar los servidores operativos de Netnod en fases de una hora para poder hacer cambios a las entradas DNS para enrutar tráfico desde los servidores de mail de la compañía hacia sus propios servidores y, usando certificados que obtuvieron rápidamente, utilizaron sus servidores como proxies para robar la información de la cuenta del atacado y su contraseña. Un ataque dirigido en la infraestructura del DNS brinda un boleto de entrada al tráfico de la víctima y está oculto, ya que lo utilizan por un periodo corto de tiempo.

Según Fältström, si bien los servidores de nombres del atacante fueron visibles para Netnod por un tiempo en Whois, el monitoreo no fue de ayuda, debido a que el software para hacerlo solo revisa esta información una vez cada cuatro horas. Lo que se hizo visible en uno de los tres ataques a Netnod fueron las fallas de DNSSEC, pero solo debido a que los atacantes olvidaron eliminar (o eligieron no hacerlo) DNSSEC en el dominio para un tercer paso del ataque, lo que significa que falló la validación. Este aspecto de DNSSEC demuestra que, si bien son es posible contramedida, DNSSEC no protege contra ataques una vez que el atacante ya tiene acceso a las credenciales del registrador y puede cambiar la información de dominio. Será interesante ver cómo cambian estos ataques en la configuración del DoH.

Bloqueo de seguridad/registro

Otra posible contramedida es bloquear los datos de registración en el registro y hacer cambios que dependan de más o menos intervenciones manuales. Esta medida es ahora tema de debate en la comunidad DNS. Durante la reunión paralela en Praga, los participantes de los registros indicaron que ofrecen bloqueos de registro (con unas pocas excepciones: .de, .ch, .br, .ua). En la

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

mayoría de los casos, los bloqueos de registro son encendidos o apagados por los registradores, que también son quienes pueden procesar los cambios mediante algún tipo de proceso manual (fax, llamada telefónica, compartición de notas y contraseñas). Algunos de los registros que se manejan de esta manera son VeriSign (.com, .net, .name, .cc, .tv.), .fr, .jp, .ca y .se. Algunos registros (.at, .cz) dependen del accionar de los solicitantes antes de procesar cambios. También está el ejemplo de un estado de dominio VIP bajo .dk, que requiere confirmación para cada solicitud de EPP para hacer cambios en la registración, haciendo que todos los cambios sean "asíncronos".

El objetivo de la reunión era considerar una posible estandarización de los procesos de bloqueo de registro ya que, actualmente, los procedimientos establecidos por los registros varían considerablemente entre uno y otro, lo que dificulta que los registradores los implementen todos. Los precios de este servicio pueden ir de cero a EUR 500.

Durante la sesión, Ulrich Wisser (.se) presentó un intento de estandarización. El draft de la RFC publica una extensión EPP que añade un paso de autorización manual dentro de EPP para proteger los cambios hechos a un objeto por parte del cliente patrocinador o su cliente. El draft de la RFC, que ahora está siendo evaluado por el WG de RegEXT, solicita "autorización adicional para comandos de transformación", usando opciones EPP en banda disponibles mediante Estándares EPP [RFC5730], [RFC5731], [RFC5732], [RFC5733].

Con un objeto del registro bloqueado, los comandos de transformación solo se pueden ejecutar si se brinda la autorización adecuada (o el objeto estaba desbloqueado fuera de banda). Hay varias preguntas abiertas que se deben resolver en el WG.

Al mismo tiempo, varios participantes en la reunión paralela solicitaron una declaración clara sobre cuál era la motivación para la estandarización ("¿Qué queremos lograr?") y sobre la terminología ("¿Qué significa "bloquear/cerrar"?). Un argumento en contra de la estandarización fue que la diversidad podría ser una característica y no un bug, ya que la diversidad podría hacer que los ataques sean más difíciles de llevar a cabo.

También tuvo lugar un debate importante sobre la necesidad de incluir una autenticación de dos pasos en los procesos EPP de manejo del dominio y de registración.

Conclusión de una víctima de DNSpionage

Un bloqueo de registro es una "herramienta extremadamente pesada", y quizás es "demasiado pesada para los negocios normales", ya que hacerle cambios rápidos es difícil y tedioso, según las conclusiones que expresó Fältström a quien escribe. Si bien reconoció que Netnod y Frobbit "no tenían todos los caballos en el establo" y que estaba en los planes la autenticación de dos pasos (y, también, el bloqueo de registro en el caso de Netnod), sugirió que la comunidad debería considerar alguna medida "que se encuentre en un punto medio entre el bloqueo de registro y nada".

Una opción que mencionó Fältström fue una notificación push a la que se puedan suscribir los solicitantes con el registro, que les advierta sobre cambios reales. Otra opción era encontrar una solución de bloqueo de registro más simple (más liviana). Los registros también podrían considerar instalar sistemas de monitoreo similares a los de las compañías de tarjetas de crédito para detectar "comportamiento anormal". Otras recomendaciones de higiene general que ya se conocen (también en los consejos del SSAC) tenían que ver con no usar texto en plano dentro

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

de la red propia, y con controlar el propio servidor de nombres (en lugar de tercerizar la tarea a un proveedor externo).

El debate sobre el bloqueo de registro continuará y el draft de Wisser está abierto a observaciones.

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

Grupos de Trabajo y reuniones BoF

WG de DPRIVE: el camino del recursivo al autoritativo sigue siendo un tema

Además de tomarse el tiempo para hablar sobre el DoH, el WG de DPRIVE debatió cómo seguir con la antigua pregunta de si deberían protegerse las consultas que viajan entre los resolutores recursivos y los servidores autoritativos. Alex Mayrhofer (nic.at) y Benno Overeinder (NLnet.labs) abordaron el tema tras varios intentos de iniciar el debate.

¿Los usuarios señalan sus deseos de privacidad?

Mayrhofer y Overeinder expusieron las cuestiones que se tratarán en un futuro draft (ver su documento de Github) y solicitaron más comentarios en Praga. Le preguntaron al grupo si debería convertirse en un documento más bien prescriptivo (los operadores deben hacer que el camino del recursivo al autoritativo sea amigable con la privacidad), o si debería presentar otras opciones. Una pregunta relacionada fue cómo lidiar con los diferentes intereses de los operadores, los usuarios y los desarrolladores. Las decisiones sobre cómo organizar la señalización de qué ofrecen/quieren las distintas partes podrían variar según las respuestas.

Otra pregunta abordada fue si el DoT sería el protocolo preferido para proteger las consultas que viajan entre los resolutores recursivos y autoritativos. El WG debatió esto brevemente y pareció llegar al acuerdo de que el DoT es la opción correcta, por lo menos por ahora. Según Mayrhofer, los aspectos funcionales del futuro draft podrían incluir mecanismos de protección de privacidad, la autenticación de servidores (cómo lidiar con servidores autoritativos no autenticados), desempeño, la detección de disponibilidad (por zona, por servidor de nombres identificado o por dirección IP), y también la propagación de políticas de usuario final.

La discusión estalló cuando llegó al tema de qué señalización podría ser necesaria y cómo deberían reflejarse los deseos de los usuarios finales. Durante el debate sobre el alcance, Mayrhofer señaló que era probable que los intereses de las diferentes partes no estén alineados. Desde el punto de vista del usuario, la confianza transitiva establecida cuando las consultas viajan a un servidor autoritativo podría ser problemática, ya que el usuario no ha tenido la "oportunidad de identificar qué datos estuvieron expuestos a qué parte autoritativa (y por qué camino)". Es posible que los usuarios quieran "estar informados sobre el estado de las conexiones que se hicieron en su nombre", según le recordaron los autores al WG, lo que también desató un debate sobre opciones posibles para permitir que los usuarios finales reciban señales sobre las decisiones tomadas.

La mayoría de los participantes claramente estaban a favor de la señalización solo para aplicaciones. La señalización para usuarios era muy difícil, según Daniel Kahn Gillmor (ACLU), y el IETF no es bueno en eso. Eric Rescorla, CTO de Mozilla, dijo que no le quedaba claro en qué resultaría una señalización de opciones para los usuarios. Otros argumentaron que, si bien sería bueno tenerla, la señalización para los usuarios finales solo debería considerarse a gran escala para poder evitar mayores demoras en la producción del documento del viaje del recursivo al autoritativo. Sara Dickinson (Sinedun) expresó que otra opción sería que los usuarios activen la

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

señalización solo cuando deseen resolución, siempre y cuando esto no exponga sus datos privados.

El debate de este documento continuará en la lista de correos. Curiosamente, Mayrhofer también preguntó abiertamente si la discusión debería llevarse en el WG de DNSOP, ya que podría ser necesario que todos los operadores DNS usen el modo de preservación de la privacidad. Sin embargo, al igual que con el debate sobre el DoH, los presidentes de DNSOP se mostraron felices de mantener el debate sobre privacidad fuera de DNSOP por el momento.

Más soluciones alternativas para la privacidad del DNS

El WG de DPRIVE debatió brevemente la posibilidad de facilitar la implementación del DoT. Manu Bretelle (Facebook) propuso la idea de usar la combinación de una infraestructura de clave pública simple especial y DNSSEC al nivel del padre para permitir que sitios inseguros participen en DoT sin estar ellos obligados a introducir DNSSEC. Dado que la firma de la PKIX viene de servidores DNS padres, los servidores que están más abajo en la jerarquía serían capaces de incorporar el DoT sin hacer el esfuerzo de desplegar DNSSEC para la autenticación. El draft de Bretelle quiere incorporar un "Registro de recursos de delegación SPKI (DSPKI)" a tal efecto. Hasta ahora, las reacciones del WG no han sido concluyentes.

El RDAP en regext IETF: ¿relacionado con la privacidad/las políticas o no?

Desde la reunión IETF 103, se publicaron las siguientes RFC: 8521, 8495, 8543 y 8544. Con otros dos documentos en camino a la revisión del IESG (Extensión de tarifa de registro y registración en paquete estricto), el WG mira al futuro y debe tomar una decisión sobre cuántos nuevos hitos asumirá en su carta constitutiva renovada. La pregunta es: ¿el RDAP debería tener su propio WG?

Debido a que, durante una reunión interina, cuatro de cinco documentos fueron elegidos para convertirse en nuevos hitos en relación con el Protocolo de Acceso a Datos de Registro (RDAP), el WG debatió si el trabajo sobre el RDAP ameritaba un Grupo de Trabajo especial para permitir que continúe el trabajo en las extensiones EPP. George Michaelson (APNIC) argumentó que el RDAP había sido relegado por mucho tiempo como solución a un problema de la comunidad, y que, con mucho trabajo por delante en el protocolo de seguimiento de Whois, tendría sentido formar un WG especial. Según varios expertos, el RDAP tendrá un impacto mucho mayor en la comunidad que el EPP, que es de interés solo para aproximadamente 20 proveedores back-end y sus 20.000 registradores.

Varios participantes en Praga estuvieron claramente en contra de la idea de dividir el trabajo, especialmente debido a que, hasta ahora, el WG siempre se ha quedado corto de expertos que revisen el draft. Al dividir el trabajo, la revisión experta se puede volver aún más difícil de lograr. Aquellos que siguen el trabajo de RegEXT son los mismos que seguirían el desarrollo de la serie del estándar del RDAP. Tras un consenso accidentado, el grupo también recomendó que el nuevo director de área, Barry Leiba, sea más flexible con los documentos asumidos (y también con la cantidad de documentos).

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

Todo RDAP, y algunas preguntas de políticas

El WG estará trabajando y tratando de estandarizar cuatro documentos relacionados con el RDAP, en particular:

- Federated authentication for RDAP
- RDAP Query Parameters for Result Sorting
- RDAP Partial Response
- RDAP Reverse Search
- Login Security Extension for EPP

La autenticación federada es un tema antiguo que Scott Hollenbeck presentó varias veces en los últimos años. El draft de Scott Hollenbeck resume cómo el RDAP llevará a cabo la autenticación de un cliente basado en navegador. El cliente RDAP (usuario OpenID) consulta a los servidores RDAP, que verifican con un Proveedor OpenID que el cliente RDAP sea auténtico. Una combinación del tóken de ID del cliente y del tóken de acceso (recibida del servidor de autorización) autentica al cliente en relación con el servidor RDAP y permite el acceso (diferenciado) (dependiendo de las políticas).

VeriSign Labs está llevando a cabo implementaciones de prueba de tres niveles. Ofrece respuestas básicas para usuarios no autenticados, y un conjunto de datos más grande para aquellos identificados mediante el mail de Google o Hotmail, de Microsoft. Además, para aquellos autenticados completamente ("usando proveedores de identidad más restrictivos", en particular https://testprovider.rdap.verisignlabs.com/ y https://www.mojeid.cz/ de CZ.NIC) se ha puesto toda la información a disposición.

Mario Loffredo, de Registro .it, presentó otras tres propuestas RDAP sobre las que el WG estará trabajando en sus nuevos hitos:

- "RDAP Query Parameters for Result Sorting" (que permite organizar y limitar los resultados de las consultas para acceso a datos, incluso los metadatos de registración),
- "RDAP Partial Response" (que permite recibir subconjuntos de posibles resultados de consultas para ahorrar ancho de banda y tiempo), y
- "RDAP Reverse Search" (que permite buscar todos los dominios relacionados con una entidad, un solicitante, un e-mail, o una dirección).

Loffredo les preguntó a los miembros del WG si les parecía que los problemas de privacidad relacionados con la búsqueda inversa habían sido abordados adecuadamente, y obtuvo, en su mayoría, respuestas negativas. Stephane Bortzmeyer concluyó que la "Sección de Consideraciones sobre Privacidad" del draft solo llegó a confirmar que se deben obedecer las leyes locales. En lugar de confirmar lo obvio ("acatar la ley"), la sección debería, al menos, describir el riesgo que conlleva la búsqueda inversa. Loffredo argumentó que, en el draft, se quería centrar en la tecnología, en lugar de lidiar con los potenciales riesgos y normas fuera del alcance del draft. Los datos de registración sensibles DEBEN estar protegidos y ser accesibles únicamente con propósitos permitidos. La sección, principalmente, subraya que "los servidores RDAP deben ofrecer la búsqueda inversa solo a aquellos solicitantes que estén autorizados según bases jurídicas" y también menciona "llevar a cabo una tarea específica definida por ley que sea de interés público" como una razón legítima o el "permiso de búsquedas inversas, que toman en cuenta solo aquellas entidades que hayan dado consentimiento explícito previo para la publicación y el procesamiento de sus datos personales". Ciertamente, continuarán los debates

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

sobre el problema de privacidad relativo a la búsqueda inversa. De hecho, la noción de que las políticas no tienen cabida en los documentos RDAP parece falaz, dada la siguiente motivación para la búsqueda inversa en el draft:

La primera objeción fue causada por los posibles riesgos de violación a la privacidad. Sin embargo, la comunidad TLD está considerando una nueva generación de Servicios de Directorio de Registración ([ICANN-RDS1], [ICANN-RDS2]), que brindan acceso a datos sensibles con ciertos propósitos permisibles y según políticas idóneas para reforzar la acreditación, autenticación, autorización, y término y condiciones de uso de datos del solicitante. Bien se sabe que tales políticas de seguridad no se implementan en Whois ([RFC3912]), mientras que sí se implementan en el RDAP ([RFC7481]). Por lo tanto, el RDAP permite la implementación de la búsqueda inversa en consonancia con los principios de protección de la privacidad.

Otros participantes, entre ellos Peter Koch (DENIC), reiteraron la necesidad de considerar más en profundidad los problemas de privacidad en el RegEXT, dado que el RDAP se ha convertido en una suerte de "registros de nombres de pasajeros" para los gobiernos. También surgió la pregunta sobre cuál debería ir primero: los requisitos desarrollados por ICANN o la implementación técnica en el IETF. Koch advirtió sobre los peligros del "lavado de políticas" a través de un WG técnico en el IETF.

Se mencionaron brevemente algunas ideas sobre un posible draft de privacidad sobre el RDAP (un documento clave), pero estas ideas podrían ser rechazadas una vez más por el mantra de "atenerse al nivel técnico".

DNSOP – DNSSEC: las cookies del servidor DNS y la "organización" del lío de los TLD especiales

Hasta ahora, el Grupo de Trabajo del DNS ha evitado abordar los debates de privacidad del DNS o DoH en sus agendas, contento de dejar que el tema se debata en DPRIVE o en cualquier otro espacio. Será interesante ver si esto cambia, dadas las solicitudes de que la BCP de la privacidad del DNS se convierta en una práctica operativa (o incluso exigida por la normativa local) para todos los proveedores DNS.

Por otra parte, mantener a raya la controversia del DoH podría ser el resultado de la reticencia de tres presidentes a sobrecargar sus agendas, que ya está bastante ocupada con drafts sobre:

- DNSSEC de proveedor múltiple (ofrece varios modelos de cómo compartir claves o cómo usar varios conjuntos de claves de proveedores DNS de un cliente),
- ejecución de instancias locales de zona raíz (también conocida como desarrollo de zona raíz hiperlocal),
- recomendaciones en contra del cambio de servidores en caso de que los servidores que validan DNSSEC fallen,
- pautas sobre el TCP como protocolo de transporte para el DNS.

Un nuevo draft en discusión es un intento de estandarización de las cookies del servidor DNS, que, hasta ahora, los programadores han construido de formas muy diversas.

Un debate que se inclina hacia las políticas y que el WG ya no puede seguir demorando es el que tiene que ver con los TLD especiales. Suzanne Woolf, copresidenta del WG, argumentó que la actual especificación de asignar dominios de nivel superior especiales para servicios que no

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

sean del DNS (como el dominio Tor, .localhost, .onion, RFC 6761) debía ser revisada o clarificada para evitar que más personas lleguen al IETF por los TLD y, así, abrir una posible vía para las personas que intenten burlar el nuevo proceso de TLD de ICANN, que es costoso y arduo. Incluso dentro del WG, no hay consenso aún sobre cómo lidiar con la RFC sobre TLD de uso especial.

En su documento propuesto, Woolf intenta brindar más pautas sobre qué podría tomarse como un nombre especial. Otra opción que consideró el WG fue ponerle punto final a la RFC y considerarla "histórica". Muchos participantes señalaron que la cooperación con ICANN es necesaria para esclarecer posibles procesos. Peter Koch (DENIC) expresó que el debate también podría requerir audiencias adicionales dentro del IETF en su totalidad.

Un exsolicitante de dominio de uso especial, el investigador Christian Grothoff, declaró que, tras ser rechazado para recibir .gns, el GNU fue claro al crear .gns como un sistema de resolución de nombres cifrado disponible en paralelo al DNS.

RG de SMART: los "datos cifrados" se quitaron de la lista de objetivos

Otro grupo que se está organizando en el IETF es el Grupo de Investigación de Detención de Malware e Investigación de Amenazas (SMART). La reunión, catalogada como una reunión de la Junta de Arquitectura de Internet (IAB), estaba repleta, quizás gracias a un invitado de alto nivel, Ian Levy, director técnico del Centro Nacional de Seguridad Cibernética (NCSC), el órgano de ciberseguridad/defensa del servicio de inteligencia británico del Cuartel General de Comunicaciones del Gobierno (GCHQ).

El NCSC ha sido un gran impulsor de la iniciativa del grupo de investigación, que en el draft original de la carta constitutiva declara que "investigará cómo se pueden cumplir los requisitos de defensa ante ataques cibernéticos en un mundo de datos cifrados". Según la nueva versión de la carta, el RG de SMART declara que "investigará los efectos, tanto positivos como negativos, de los protocolos existentes, propuestos y recientemente publicados y de los estándares de Internet en la defensa contra ataques". Según Kirsty Paine (NCSC), el objetivo principal es que los diseñadores, implementadores y usuarios de nuevos protocolos estén mejor informados y que el RG de SMART se convierta en "la autoridad" de consulta en materia de defensa ante ataques en el IETF/IRTF para los desarrolladores.

En su presentación (que fue la última de una agenda de SMART bastante ocupada), Levy promocionó el trabajo de su agencia (elabora recomendaciones, informes anuales para mejorar la seguridad; intenta facilitar el "uso de la ciberseguridad" por parte los usuarios; desarrolla etiquetas rojas-amarillas-verdes para productos IoT; e impulsa la adopción de DMARC en la administración del Reino Unido). Otro proyecto se basa en crear una plataforma de pares de BGP para los ISP británicos para evitar hackeos al BGP, ya que este era peor de lo que dejaba ver su reputación. La agencia, finalmente, bloqueó una gran cantidad de consultas DNS de agencias públicas del Reino Unido (450.000 WannaCry, miles de Conficker).

Seguridad incompatible con la resiliencia

Levy expresó que la seguridad estaba cada vez más incorporada en los protocolos y advirtió que el cifrado no es lo mismo que la seguridad. "Cifrar algo no quiere decir que lo haga seguro", manifestó. El TLS, por ejemplo, e iniciativas como "let's encrypt" están muy bien, pero "recordemos siempre que los malos también usan lo que brilla". Los desarrolladores, por lo tanto,

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

necesitan buena información cuando toman las decisiones de no habilitar nuevos modos de ataques. La seguridad, la privacidad y la resiliencia son diferentes. Si no se hace correctamente, la seguridad y la resiliencia son incompatibles. SMART, por lo tanto, es importante desde el punto de vista del NCSC.

Daniel Kahn-Gilmore, de ACLU, reconoció que el IETF necesitaba muchos más debates sobre fallas de interfaz de usuario y la gente de interfaz de usuario necesitaba ir al IETF para informar qué señales necesitan. Al mismo tiempo, obligar a los proveedores a cooperar con los servicios de inteligencia y aplicación de la ley podría "ser usado por los malos también", al igual que otros usaron los "brillantes" protocolos de seguridad. En este sentido, Kahn-Gilmore también preguntó cuáles eran las intenciones de Levy con la llamada "propuesta fantasma", una propuesta en la que Levy y su colega, el director técnico del GCHQ, proponen permitir a las agencias de inteligencia convertirse en una parte "silenciosa" en conversaciones cifradas con targets específicos.

Levy le dijo a quien escribe que está de acuerdo con la ACLU en que no sería bueno tener un depósito de claves centralizado para el cifrado. Sin embargo, había que resolver el problema básico de cómo pueden llegar los servicios de inteligencia a la comunicación cifrada.

Primer documento draft en SMART

El WG también debatió brevemente su primer documento draft, un draft extenso sobre las capacidades y limitaciones de la seguridad en el extremo. Según Arnaud Taddei de Symantec, de 275 tipos de ataques, solo 32 se pueden detectar en el extremo. El argumento de que el control por parte de los operadores de red es indispensable surgió en varias discusiones recientes sobre los nuevos protocolos (por ejemplo, TLS 1.3 o QUIC). Se espera que el draft funcione como primera referencia sobre vectores de ataques para los desarrolladores de protocolos.

La BoF más rara: logos de marcas validadas en e-mail

La idea no fue bien recibida en el IETF, pero igual se llevó a cabo una BoF de dos horas para debatir una propuesta de varias compañías de EE. UU., incluidas Valimail, Agari y el proveedor de red Comcast, para permitir que los dueños de importantes marcas publiquen indicadores de marcas para los dominios y los usen para la autenticación, en base a estándares existentes como la Autenticación de Mensajes, Informes y Conformidad basada en Dominios (DMARC). "Si tanto el e-mail como el logo se autentican, el receptor agrega un encabezado al mensaje, que puede ser usado por el MUA (Agente de Usuario de Correo) para determinar el indicador de marca preferido del dueño del dominio".

La aseveración del logo gráfico del dueño de la marca se realiza mediante la publicación de un registro de texto en el DNS ("default._bimi.example.com"). La autenticación del registro se lleva a cabo mediante una verificación usando una autoridad de certificación (del mismo modo en que se verifican los certificados TLS).

Sus defensores argumentaron en Praga que BIMI podría impulsar la adopción de estándares de autenticación de e-mail, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) y DMARC, que brindan mecanismos para la autenticación a nivel de dominio para mensajes de correo electrónico. La adopción de estos estándares, hasta ahora, ha sido lenta, y que los BIMI usen los mecanismos podría cambiar eso. Durante el debate, Seth Blank dijo que el draft de

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

BIMI pretendía “brindar mecanismos para prevenir los intentos de dueños de dominios maliciosos por representar mensajes de manera fraudulenta desde sus dominios como si se originaran con otras entidades”.

La mera idea de que el mecanismo utilizado por los dueños de marcas importantes podría comercializarse como una herramienta antiphishing fue rechazada en la sesión BoF porque el mecanismo no funcionaría, debido a que la autenticación basada en dominios y CA solo permitía que una parte tenga control sobre un determinado dominio, en el mejor de los casos. El hecho de que no había disponible una base de datos central y reconocida para los derechos de propiedad intelectual relevantes —y los DPI se disputaban en todo el mundo y en muchos aspectos— fue otra objeción que surgió durante la sesión.

Los autores se distanciaron de anuncios previos relacionados con que el antiphishing era el objetivo. Sin embargo, sí reconocieron que la propuesta tiene varios problemas, en particular que el concepto de logo gráfico era solo para dueños de marcas importantes (que son propietarios de tales logos y son capaces de hacer las inversiones necesarias para propagar sus logos a través de la estructura BIMI). Los autores también enumeraron varias preocupaciones de seguridad bastante serias (ver también la extensa sección sobre seguridad en el draft general). Se puede hacer uso y abuso del logo fácilmente como bug web para rastrear usuarios, se podría ocultar malware en el “payload” o en imitaciones de logos (similares a los de las grandes marcas).

Hubo un fuerte consenso respecto de que se podría engañar a los usuarios para que piensen que, con la visualización de los logos, sus e-mails serían más seguros. Varios desarrolladores, incluido David Schinazi (Google), instaron a la comunidad IETF a nunca estandarizar tal mecanismo. Curiosamente, según comunicados de prensa previos, Google había sido uno de los que apoyaba el proyecto (“BIMI es una iniciativa de los tres proveedores de correo más importantes Microsoft, Google y Oath [Verizon, AOL, Yahoo] y también de Comcast, Agari, RP, Valimail y PayPal”). Los defensores de BIMI expresaron que estaban pensando cuáles serían los próximos pasos y probablemente solicitarían otra BoF.

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

Noticias del IETF

El Comité de Supervisión Administrativa del IETF (IAOC) es historia. En la reunión IETF 104, la comunidad IETF tuvo la primera oportunidad de conocer a los nuevos miembros del consejo de la LLC. Tras los pasos del IETF para convertirse en una organización jurídicamente independiente (a cargo de contratar y recaudar fondos fuera de la ISOC), los miembros de la LLC se reunieron durante la semana del IETF en Praga. Los miembros son:

- Maja Andjelkovic
- Alissa Cooper
- Jason Livingood, Presidente
- Sean Turner, Tesorero
- Peter Van Roste

Las agendas y minutas del consejo de la LLC se pueden ver aquí. Algunos de los puntos interesantes en la agenda IOC actual de la LLC incluyen la búsqueda de un director ejecutivo y la planificación del presupuesto.

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