INFORME IETF 88

Vancouver

4 al 8 de noviembre de 2013

Monika Ermert
para

CENTR &
LACTLD

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

LACTLD agradece la colaboración de CENTR por los aportes fundamentales para el financiamiento de la iniciativa, así como el apoyo de ISOC y la contribución de Hugo Salgado así como la de Arturo Servin y Carlos Martínez en este informe. Para acceder a la versión en inglés de este informe:
http://www.centr.org/CENTR-Report-IETF88

LACTLD
Latin American and Caribbean ccTLDs Organization

Índice

Destacados

Un IETF más politizado

Es posible que la reunión del IETF en Vancouver haya sido la más politizada de los últimos tiempos. Las revelaciones de Snowden, de las que se había hablado apenas y cautelosamente durante el encuentro en Berlín en agosto, llevaron finalmente a un gran debate en el órgano de estandarización por distintas razones. En el futuro, sin duda se hablará de Vancouver por la exhortación (uno debería decir, el voto sonoro) a la encriptación. Para algunos, la conclusión general fue directamente "IETF – TLS". Sin embargo, en un sentido más sutil, la reunión también podría ser recordada como el comienzo de un IETF más politizado, como demuestra la pregunta sobre la organización de su "representación" en foros tales como el Foro de Gobernanza de Internet de las Naciones Unidas (IGF por sus siglas en inglés).

Representar al IETF

Le tocó al ex-presidente del Consejo de Arquitectura de Internet (IAB por sus siglas en inglés) hacer esta pregunta durante la sesión dedicada a la gobernanza de Internet (que seguro que no será la última sobre este tema, considerando los hechos): cómo harán los líderes del IETF para poner en marcha un proceso que resulte en posturas consensuadas antes del viaje del presidente Jari Arkko a la Conferencia Internacional sobre Gobernanza de Internet, a realizarse en Brasil poco antes del próximo encuentro del IETF (que será en Londres en marzo del año próximo), o a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones. Además de otorgar el poder de representación a los líderes del IETF y el IAB, también debería brindarse un canal de comunicación con el IETF a otros, según el experto en el IETF Scott Bradner.

En esa misma sesión, Arkko reconoció la creciente presión política ejercida sobre la comunidad técnica, por ejemplo, sobre la comunidad de los ccTLD, en algunos países. "Tenemos que conversar más con el resto del mundo, tenemos que elaborar una opinión y ser capaces de presentarla", reconoció. Por ello, el IETF debe identificar áreas en las que el consenso es sólido. Andrew Sullivan, uno de los "no representantes" **del IETF en el IGF de Bali,** afirmó: "Como comunidad, tenemos que tener una idea bastante clara de lo que queremos, si no, otros decidirán por nosotros." Un representante de Anatel se pronunció en contra de la noción de interferencia gubernamental, y dijo que la cumbre de Brasil era un intento de ocuparse de desequilibrios que tienen ya una larga historia y, por ejemplo, de la internacionalización de ICANN. El IETF, por cierto, era parte del sistema de gobernanza de Internet.

Queda pendiente una verdadera respuesta acerca de cómo proceder. Por el momento, se señaló la necesidad de seguir conversando sobre la **lista de correos del IAB** (también se hizo referencia a la **taxonomía de la ISOC para desafíos de gobernanza**). Dado que se trata de un foro de estandarización que no es una asociación constituida, sino que usa la Internet Society (ISOC) como su entidad social hacia el exterior (con la Fundación del IETF para cubrir ciertos aspectos legales para la comunidad), sus líderes son considerados "pares", no representantes. Será interesante ver como se expresa el "consenso aproximado" (rough consensus) en foros más formales de políticas públicas.

Incluso Bruce Schneier, una de las celebridades invitadas, se refirió al desafío planteado por la capa 8, y advirtió: "Tenemos que elaborar un nuevo modelo de gobernanza de Internet, que hasta ahora ha sido gestionada por el gobierno de EE UU bajo la percepción generalizada de que respondía a los intereses de todos. Eso ya pasó. Y tiene que ser una buena solución, porque si no se hará cargo la UIT". Chris Disspain

(auDA) y Lynn St. Amour (presidente saliente de ISOC) dijeron que al debilitarse la alianza natural con EEUU, es posible que el grupo I* tenga que intervenir.

Vigilancia, vigilancia, vigilancia

Después de un debate por momentos acalorado en la sesión plenaria sobre vigilancia generalizada, el presidente del IAB, Russ Housely (Vigil Security, consultor de la NSA) pidió un voto sonoro para **cinco compromisos/afirmaciones diferentes:**

1. el IETF está dispuesto a responder al ataque de vigilancia generalizada;

2. la vigilancia generalizada es un ataque, y el IETF debe adaptar su modelo de amenaza para tenerla en cuenta cuando elabora las especificaciones para que un protocolo pueda convertirse en estándar (standard track);

3. el IETF debería incluir la encriptación, incluso sin autenticación, cuando sea práctico;

4. el IETF debería realizar un esfuerzo para implementar la encriptación de punta a punta, incluso cuando hay dispositivos intermedios en el trayecto (reacciones positivas y negativas, pero la mayoría a favor);

5. actualmente se utilizan muchos protocolos inseguros en Internet, y el IETF debería crear una alternativa segura para los más populares (la mayoría opinó que sí, pero algunos que no).

Las primeras tres fueron adoptadas por unanimidad. La cuarta y la quinta, cuestiones más prácticas, recibieron algunos votos negativos, pero igual fueron declaradas de consenso aproximado. El método de votación fue cuestionado por algunos participantes, y el debate acerca de lo que algunos definieron como simplemente "teatro político" o "teatro sonoro" todavía no ha terminado. Sin embargo, es evidente que una mayoría amplia se sintió urgida a dar una respuesta general, desde la perspectiva de la comunidad técnica, a las revelaciones sobre vigilancia masiva y elusión "maliciosa" de todas las medidas de seguridad elaboradas y recomendadas por el IETF.

Si bien la encriptación absoluta de las comunicaciones no hará a los protocolos 100% seguros, sí haría casi imposible el "análisis pasivo". Actualmente la NSA espía y almacena todo lo que ocurre. En el futuro con encriptación no podrán espiar todo, pero sí podrán buscar objetivos específicos y atacar ciertos usuarios. De acuerdo a las conversaciones entre expertos, de todas formas es una ganancia, ya que hay legislación que autoriza a ciertos organismos a espiar en forma selectiva, con alguna orden judicial de por medio y por razones de seguridad. Lo que todos están de acuerdo es que es muy malo el "espionaje a granel".

Fue justo antes de la reunión del IETF en Vancouver que se supo la noticia de la intervención de las conexiones internas entre los centros de datos de Google en los cuales no se había encriptado el tráfico. **"Que se vayan a la mierda"**, escribió uno de los ingenieros de Google responsables de proteger la red de la empresa, en un posteo personal que anunciaba los pasos para encriptar ese tráfico. El IAB/IETF invitó a Bruce Schneier a la reunión de técnicos para escuchar declaraciones igualmente jugosas sobre los programas de la NSA.

Schneier, acerca de la NSA

Schneier, quien ayudó a The Guardian a revisar y evaluar miles de documentos provistos por Snowden, no tenía ninguna razón para ser diplomático: "La NSA ha convertido Internet en una plataforma gigante de vigilancia", afirmó. Habiendo examinado las largas listas de programas especiales – desde las recolecciones masivas más obvias, organizadas bajo órdenes judiciales vinculadas con la Ley de Vigilancia de Inteligencia Extranjera, hasta la intervención grosera de las fibras y todo tipo de subversión de estándares de encriptación – también advirtió que los esfuerzos de la NSA son "política, legal y técnicamente sólidos". El experto en

criptografía anunció, además, que "queda mucho, mucho por venir", pero que algunas de las tácticas de la NSA nunca saldrían a la luz "porque en los documentos no hay nombres de empresas ni listas de estándares de cifrado comprometidos".

La recomendación de Schneier fue utilizar la encriptación siempre que sea posible, ya que las soluciones políticas, si fueran factibles, solo podrían darse en el largo plazo. También subrayó que la vigilancia generalizada es, en gran medida, un "subproducto de la sociedad de la información". Las computadoras crean y almacenan datos y posibilitan su búsqueda, y el resultado es "vigilancia generalizada, vigilancia hacia atrás en el tiempo, pérdida de las conversaciones efímeras, sistemas que nunca olvidan". Y, por cierto, Schneier está seguro de que no es que la NSA se despertó una mañana y dijo, espiemos a todos. Más bien, "miraron a su alrededor y dijeron, guau, las corporaciones están espiando a todo el mundo, consigamos una copia".

Es un ataque

"Es un ataque", fue la conclusión desapasionada del Director del Área de Seguridad del IETF, Stephen Farrell (un especialista en computación científica del Trinity College de Dublín). "Olvídense de los motivos, de las cuestiones políticas. Si observan las acciones de la NSA y sus socios, ya sea bajo coerción o no, se trata esencialmente de una forma de ataque multifacético". En una entrevista, Farrell rechazó la posibilidad de complicidad de los ingenieros, pero reconoció que con más imaginación, quizá, la comunidad podría haber descifrado el rompecabezas de la vigilancia. El Director del Área de Seguridad en Berlín había empezado a responder de manera práctica a las revelaciones mediante la creación de una lista de correos "perpass", que condujo a la organización de un BoF en Vancouver en el cual se presentaron posibles respuestas técnicas al ataque "multifacético". (Para más detalles, véase también el área de aplicaciones, httpbis y, además, la abiertamente declarada pérdida de confianza en el proceso de estandarización de cifrados del NIST que se relata más abajo.)

Todavía se está llevando a cabo un debate fundamental: dónde poner el límite con respecto a la encriptación. ¿Debería realizarse siempre que fuera posible (encriptación oportunística), o debería ser obligatoria (lo cual llevaría al fracaso de la comunicación no encriptada)? ¿Debería ser solo encriptación con autenticación, o la encriptación sin autenticación (cuando esta última no fuera posible) podría ser suficiente? Durante la entrevista, Farrell dijo que la comunidad técnica había fallado, en cierto modo, al presionar para establecer el estándar más alto posible en lugar de permitir una implementación paso por paso. La buena seguridad cuya implementación sea factible es un hueso duro de roer, afirmó el presidente Arkko.

A pesar del amplio consenso sobre la necesidad de mayor y mejor encriptación, también se expresó preocupación acerca de las consecuencias de este tipo de carrera armamentística. Harald Alvestrand, ex-presidente del IETF, consideró que esto permitiría a los malos protegerse también. Sin embargo, reconoció que, dada la situación, no había otra opción que proteger todo el tráfico. Vale la pena, suspiró.

Provisión de estándares para ICANN. De una base de datos Whois agregada, a una federada y centralizada

La sesión sobre gobernanza de Internet también incluyó a Chris Disspain, Director General de auDA y miembro del grupo de trabajo de expertos de ICANN que se ocupa **de servicios de directorios de registros de gTLD de próxima generación.** Este grupo de trabajo, según Disspain, se estableció en un esfuerzo por repensar el

"problema" de Whois después de reconocer e implementar las recomendaciones del equipo de evaluación de Whois de ICANN, uno de los cuatro equipos de evaluación establecidos por el Compromiso de Afirmación (AoC por sus siglas en inglés).

Whois ha sido un tema candente desde la reunión de ICANN en Montreal, debido a las quejas, provenientes principalmente de autoridades de seguridad anglosajonas, y de la comunidad de titulares de derechos de propiedad intelectual, acerca de la inexactitud y falta de confiabilidad de los datos de Whois. A partir del informe del Equipo de Evaluación y de un documento del Comité Asesor sobre Seguridad y Estabilidad de ICANN, las nuevas autoridades de esta organización decidieron recomenzar el trabajo sobre este tema con el objeto de elaborar una propuesta completamente nueva.

Disspain informó que luego de muchas críticas a la "base de datos de registros agregados" que se había sugerido, el grupo de expertos cambió su propuesta por un **"modelo federado".** La información no se almacenaría en una base de datos central; solo el acceso a los datos de registro se realizaría a través de esa plataforma. Si bien la idea es atractiva desde el punto de vista de los registradores (no se producirían más llamadas de fuerzas de seguridad extrañas), podría llevar a otro conflicto jurisdiccional. El acceso a través de un futuro portal centralizado en EE UU será reglamentado por la legislación de ese país, y los registros de otros países podrán regular el acceso a los datos personales de otra manera. ¿Será posible limitar el acceso (por parte de terceros países) a los datos recolectados en jurisdicciones más estrictas en temas de privacidad? ¿O solo la limitación de lo que se recolecta en primer lugar determinará el envío de respuestas vacías? ¿O acaso los registros tendrán que formular políticas complejas de acceso (permitírselo a algunas investigaciones de algunos países)?

¿El proceso de elaboración de políticas y la estandarización técnica en sincronía?

El IETF no estuvo involucrado en ninguna de estas cuestiones vinculadas con políticas, afirmó Murray Kucherawy [Facebook, presidente del **GT Weirds** (Servicio Extensible de Datos de Registro en Internet)]. La elaboración de un nuevo protocolo técnico (Weirds) se hizo necesaria no solo por la reforma de Whois realizada por ICANN, sino también por el paso dado por los registros de direcciones de IP para brindar "datos whois limpios" también para los recursos de numeración.

El GT sobre Weirds y el grupo de expertos de ICANN sobre el registro de próxima generación trabajan en paralelo, según Disspain, con el acuerdo de que ICANN se centra en principios de diseño y el IETF en el protocolo técnico. Los principios de diseño que Kucherawy resumió en Vancouver son los siguientes:

1. internacionalización;

2. una sintaxis de respuesta específica;

3. la posibilidad de redirigir;

4. autenticación (permitir los tan ansiados servicios diferenciados, según los cuales a las fuerzas de seguridad/los dueños de IPs/las partes interesadas legítimas les correspondería más que a las personas comunes);

5. un estándar único para nombrar y numerar recursos;

6. eliminación de la necesidad de un cliente especial; y

7. el uso de http (arquitectura REST, transferencia de estado representacional) para Whois.

Las **pruebas de interoperabilidad** para las implementaciones de Weirds de los registros de números y de VeriSign, por ejemplo, ahora se realizan regularmente antes de las reuniones de ICANN. Los registros regionales de Internet (RIR por sus siglas en inglés) han empezado a elaborar un inventario de objetos para las distintas categorías. Los objetos documentados todavía no cubren todos los almacenados, por ejemplo, en RIPE. Otro tema que se conversó en la sesión del GT sobre Weirds fue si en caso de consultas sobre dominios que no forman parte del ASCII (siglas en inglés de Código Estándar Estadounidense para el Intercambio de Información), deberían entregarse conjuntos de variantes.

En este momento, los procesos de elaboración de políticas (PDP por sus siglas en inglés) de ICANN vinculados con Whois son **el PDP sobre el "thick Whois"**, el **PDP sobre privacidad y servicios proxy y el PDP sobre traducción y transliteración de datos de registro internacionalizados**, pero podría haber más. ICANN realizará una sesión de revisión de sus iniciativas vinculadas con Whois durante su próxima reunión (pueden encontrar una visión global del panorama, bastante confuso, de **políticas sobre Whois aquí**). Se señaló que, con todo el trabajo que se está realizando en paralelo, varios esfuerzos por reformar Whois fracasaron. El más reciente, IRIS (siglas en inglés del Servicio de Información sobre Registros de Internet), que podría haber permitido un acceso más nivelado, fue considerado excesivamente complejo.

Durante la sesión sobre gobernanza, no hubo gran debate acerca de qué debería privilegiarse, si la estandarización o la elaboración de políticas. En su respuesta a una pregunta sobre el cronograma, Disspain afirmó que un posible PDP elaborado por el grupo de trabajo de expertos sobre los nuevos servicios de directorio de los registros de gTLD no empezaría hasta que tuviera lugar una última discusión en la reunión de ICANN en Singapur, y luego de que la junta tomara una decisión. Esto le daría algo de ventaja al IETF.

Este tipo de intercambio de alto nivel entre ICANN y el IETF (el presidente y director general de ICANN, Fadi Chehadé, presenció la sesión en silencio) es una novedad, pero puede ser que se profundice durante la reunión del IETF en Londres el año próximo, de la que ICANN será anfitrión.

GTs y BoFs

BoF sobre Perpass (Manejo del monitoreo excesivo): Distribuir el presupuesto de los observadores

El BoF sobre Perpass intentó abarcar algunos de los temas vinculados con el análisis de amenazas y enumeró algunas áreas de trabajo posibles, pero no alcanzó resultados concluyentes. Quizá se haya alcanzado un consenso aproximado (muy aproximado) en uno de los puntos debatidos: encarecer las operaciones de vigilancia, y obligar a los atacantes sofisticados que poseen fondos considerables a concentrarse en blancos específicos. El espionaje dirigido a blancos individuales no desaparecerá, pero el dirigido a grandes grupos puede frenarse, afirmó Schneier.

El único tema general que no se trató en otros GTs fue el de la privacidad. El IETF empezó a considerar este tema hace algún tiempo, y se le encargó a la dirección de seguridad la investigación de posibles amenazas a la privacidad en el caso de los nuevos protocolos. Alissa Cooper (Center for Democracy and Technology), una de las promotoras de este trabajo en el IETF, **detalló una nueva "buena práctica actual" (BCP** por sus siglas en inglés) que aspira a hacer que la "minimización de datos personales" y la "encriptación de datos privados enviados a través de la red" con encriptación oportunista se conviertan en "requisitos mínimos" para los

nuevos protocolos que entran en el proceso de estandarización. Solo en circunstancias excepcionales (eliminación o daño severo de la función prevista) podría eliminarse este requisito.

Un aumento de la privacidad y de la encriptación, o la exigencia más estricta de privacidad y encriptación, será, en cierta medida, enemigo de las mediciones. La industria a cargo del monitoreo y las mediciones, a la vez, debe tomar consciencia de que sus propias herramientas fueron utilizadas para vigilar, según el académico Brian Tremmall (ETH Zurich).

Durante la sesión, Dave Thaler (Microsoft) enumeró los posibles puntos de ataque, que superan considerablemente los esfuerzos de control de la red. Esta es la lista de Thaler:

1. compromiso de raíces y autoridades de certificación, por ejemplo, DigiNotar y Flame, y de herramientas de depuración como add root;

2. creadores y distribuidores de software (generadores de números aleatorios débiles, comprometer CryptoAPIs);

3. explotar las debilidades de software para usuario final de uso extendido, instalación de puertas traseras;

4. repositorios de datos (servidores de correo electrónico, servidores web);

5. diseñadores de protocolos y algoritmos (influir sobre las soluciones);

6. operadores de redes;

7. fibra física, torre inalámbrica, satélite, etc. (intervenciones);

8. diseñadores y fábricas de hardware (puertas traseras, troyanos).

Se puede acceder a las **actas detalladas aquí** para ver la discusión completa. Para obtener una actualización del grado de avance del trabajo, véase el documento vivo de Stephen Farrell.

El DNS y la vigilancia

Desde que terminó el encuentro del IETF, se publicaron varios documentos preliminares que describen cuestiones vinculadas con la privacidad y confidencialidad del DNS. Uno es un planteamiento del problema, escrito por Stephane Bortzmeyer (Afnic). Otro, de Peter Koch (Denic, presidente de DNSOP: Operaciones del Sistema de Nombres de Dominio), describe cómo puede **fugarse la información de los servidores del DNS.** Otra propuesta, proveniente de los programadores del proyecto Tor, pide que haya cinco pseudo-TLDs de uso especial: ".gnu", ".zkey", ".onion", ".exit" y ".i2p". Los nuevos TLDs se "relacionarán con sistemas P2P que, dado su diseño descentralizado, no necesitan una autoridad central para registrar nombres". Ninguna de estas propuestas ha sido discutida a fondo hasta ahora, y la última es, sin duda, un proyecto bastante ambicioso.

El GT sobre el DNS debatió una lista **relativamente larga de temas**, cuya discusión está en curso pero no ha finalizado aún, además de dos nuevos (acta detallada). Se produjo un breve intercambio acerca de una nueva posibilidad de enviar **al padre datos publicados en el hijo**. La principal pregunta del documento preliminar de Hardacker sobre hijo-padre es **por qué hacen falta mecanismos adicionales**. Evan Hunt y Mark Andrews

propusieron otra opción para actualizar los padres. Joe Abley presentó una vez más lo que llama el "botón de alarma" para registradores del DNS, que permitirá desencadenar el vaciado de la memoria caché del DNS.

Se creó una nueva lista de correos para gTLDTech con el fin de alentar el debate sobre nuevos TLDs y cuestiones técnicas.

AppArea (Área de aplicaciones): Control de seguridad para algunos de los principales protocolos

Una buena parte de la reunión del Área de Aplicaciones estuvo dedicada a una revisión rápida de la seguridad de los principales protocolos de aplicaciones, desde correo y voz hasta web y jabber. La comunidad de XMPP (Protocolo extensible de mensajería y comunicación de presencia) empezará a implementar TLS (seguridad de la capa de transporte) plenamente en su protocolo. Desde el 19 de mayo, los operadores y programadores del XMPP utilizarán solamente el XMPP encriptado. La declaración de principios "Una declaración pública sobre la encriptación ubicua en la red de XMPP", aprobada recientemente en una cumbre en Seattle, fue presentada al GT de AppArea por Peter Saint Andre: "Es nuestro deber para con nuestros usuarios, aunque ellos no lo sepan, encriptar todo su tráfico".

Los compromisos establecidos en la Declaración de XMPP incluyen:

1. la obligación de ofrecer STARTTLS;

2. preferencia por la versión más reciente de TLS, 1.2;

3. obsolescencia de versiones más viejas y menos seguras de SSL (capa de conexión segura);

4. elección de confidencialidad directa;

5. preferencia por la encriptación autenticada (con encriptación oportunística como recurso alternativo);

6. transparencia con los usuarios respecto de las condiciones de encriptación de una determinada conexión cliente-servidor o servidor-servidor, de la versión de TLS y de conjunto de cifrado (cipher suite) utilizados y de los detalles y cambios del certificado;

7. conexiones obligatorias para servicios, tanto de cliente a servidor como de servidor a servidor.

La seguridad adicional tiene un costo: a partir del 19 de mayo, los usuarios de XMPP no podrían conectarse con Google Talk debido a las nuevas restricciones. Saint Andre pronunció una dura declaración sobre la necesidad de avanzar en este tema. La comunidad, los ingenieros, tiene que "ponerse las pilas" después de años de no promover una seguridad más estricta. Existe un acuerdo implícito, afirmó Saint Andre, de que no todos pueden actuar con tanta facilidad como la gente de Jabber, que eran pocos y podían darse el lujo de probar y, si la experiencia era demasiado dolorosa, retroceder. El cronograma y la experimentación rigurosos del XMPP permitirían a otros examinar más detenidamente la exigencia de utilizar TLS.

En cuanto al SIP (Protocolo de iniciación de sesiones), Jon Peterson no tiene muchas esperanzas de que se lo refuerce. Sus especificaciones básicas ya prevén el uso de TLS y S/MIME (Extensiones seguras multipropósito al correo de Internet), pero ha sido poco implementado. La seguridad era floja, afirmó. En el caso del correo electrónico, es muy difícil encontrar una forma de encriptarlo y autenticarlo de punta a punta. Muchos dicen que es mejor empezar por lo más fácil.

HTTPBis: TLS o no, esa es la cuestión

Sentarse sin hacer nada y esperar que https se convierta en el estándar de hecho ya no es una opción para el GT de httpbis. En la reunión en Vancouver, se discutió intensamente acerca del camino a seguir: elegir la encriptación oportunística y permitir la absorción rápida de la encriptación no autorizada, o exigir TLS para http 2.0.

El presidente, Mark Nottingham, propuso una nueva "versión relajada (una concesión)" de TLS que permitiría elegir una opción de control alternativa a la validación completa de certificados. La encriptación sin autorización al menos ayudaría a proteger contra atacantes pasivos. Kucherawy le recordó a los participantes que la versión de TLS obligatorio para http 2.0 ya había sido descartada. Pero algunos miembros argumentaron que luego de las revelaciones de Snowden, esa decisión tenía que ser repensada, y TLS debía ser el único estándar. El argumento de que la encriptación oportunística bloquearía el grueso de los ataques por parte de un Estado – que se basan en el monitoreo pasivo – no tiene validez, afirmaron Keith Moore (experto en SMTP) y Ted Hardie (ex-miembro del IAB), quienes participaron en el GT.

Otros advirtieron que la obligación de utilizar TLS lentificaría la migración a http 2.0. Richard Barnes (BBN) señaló que el sistema actual de certificación podría verse demasiado exigido y perder (aún más) calidad si todos necesitaran un certificado. Dane, que proporcionaría auto-certificados a través de la raíz DNSsigned, no constituye una alternativa en este momento debido a la falta de implementación de DNSSEC. Paul Wouters **presentó una propuesta** para utilizar Dane para IPSec (Protocolo de seguridad de Internet) oportunísticos durante la reunión del Área de Seguridad. No se tomó ninguna decisión respecto de qué camino tomar. Los votos sonoros expresaron divergencias. ¡Presten atención a la lista de correos!

Área de Seguridad: Pérdida de confianza en el proceso de estandarización de cifrados del NIST

Una discusión importante que se desarrolló en la reunión del Área de Seguridad en Vancouver trató la relación del Instituto Nacional de Estandarización (NIST por sus siglas en inglés) con el IETF. Los estándares de cifrado desarrollados por NIST, que se originaron en competencias como, por ejemplo, el desarrollo más reciente de Sha3 (Keccak), habían sido adoptados como estándares en los protocolos del IETF. Debido a la reapertura del NIST SP 800-90A, y el reconocimiento concomitante de que una parte del estándar había sido debilitado por la NSA, las relaciones entre los dos organismos se volvieron delicadas.

La NSA, el NIST y el IETF

Polk, que fue director del Área de Seguridad del IETF durante algún tiempo, reconoció en Vancouver que la NSA había interferido y presionado para que se incluyera su propio generador de números aleatorios en el estándar casi terminado, como alternativa a las otras tres opciones de aleatorización. Además, si bien el NIST le había pedido a la NSA ("que es una de nuestras partes interesadas") que considerara publicar su propia versión, había dado marcha atrás "porque ellos ya habían empezado a incorporarlo a sus sistemas". "No queríamos perjudicar a una de nuestras principales partes interesadas". Sin embargo, Polk negó rotundamente que se hubiera tratado de un caso deliberado de inclusión furtiva. Antes bien, fue algo típico del "desagradable proceso cotidiano de negociación".

Sus declaraciones no resultaron convincentes para todos. El ex-presidente del Área de Seguridad Sam Hartmann cuestionó a Polk, diciendo que nadie podía negar que el NIST era vulnerable a la presión de los organismos gubernamentales estadounidenses, es decir, de las partes interesadas. Un ingeniero de Intel le preguntó a Polk por qué, después de las revelaciones vinculadas con el NIST, el IETF querría continuar usando los estándares de ese organismo en lugar de buscar un foro más neutral.

Un representante de Mozilla anunció que en un año más, el proyecto utilizaría un conjunto de cifrado y un estándar de encriptación de curva elíptica propios, y acogería con agrado una evaluación por parte del NIST. Este procedimiento invertiría el proceso actual: en lugar de que los organismos de estandarización y las empresas utilizaran los productos del NIST (evaluados por la comunidad de criptógrafos), sería al revés.

Evaluación del NIST: ¿Solo de EE UU o internacional?

Polk, quien, además de haber dirigido el Área de Seguridad, hace mucho que participa en el IETF, anunció en una presentación que el NIST no se limitaría a la reapertura del SP 800-90A ni, si fuera necesario, de otros estándares para permitir un proceso de escrutinio por parte de la comunidad. El organismo también impulsaría una revisión de sus procesos para blindarlos, en un esfuerzo por recuperar la confianza.

Luego de una evaluación interna de las distintas iniciativas de estandarización para los estándares criptográficos actuales, el organismo establecería un equipo evaluador externo para investigar el tema de las posibilidades (o los casos reales) de manipulación del proceso. Si bien no está claro todavía si será un equipo internacional o estadounidense, parece haber una tendencia dentro del NIST a que sea internacional: los estándares del NIST, como el Sha, son utilizados por empresas en todo el mundo.

El IAB y el IETF exigieron una evaluación del proceso en una carta del 23 de octubre que pedía más transparencia y apertura. La carta urge al NIST a adherir a los siguientes principios:

1. hacer disponibles para el público en su sitio web todos los comentarios recibidos (incluyendo los nombres de los autores y su afiliación), provenientes de fuentes de los EEUU o de otros gobiernos o partes, de manera que sean fáciles de buscar;

2. establecer un periodo de tiempo para responder a los comentarios a fin de que los evaluadores puedan hacerlo durante el periodo inicial de comentarios;

3. brindar un resumen de los comentarios recibidos y su disposición;

4. proporcionar una explicación detallada y sustancial de los cambios resultantes de la evaluación interna (incluso en casos en los que no se dio curso a comentarios del público);

5. considerar el diseño de un proceso de apelaciones.

A pesar de los cuestionamientos, Polk parecía seguro de que el NIST podría recuperar la confianza del público. Aparentemente, el funcionario cree que la experiencia y los conocimientos especializados del organismo lo convierten en un competidor difícil de vencer. No obstante, el resultado de la evaluación y la aparición de nuevas revelaciones pueden hacer que el NIST se encuentre en dificultades para promover su neutralidad. Schneier, el experto en criptografía, dijo que aun cuando a la NSA pudiera convenirle utilizar cifrados de curva elíptica y, quizá, prefiriera orientar a la gente hacia los cifrados que mejor conoce, estaba descifrando encriptaciones fuertes mediante el robo de claves. En 1996, en el momento más crítico de las deliberaciones gubernamentales acerca de la limitación del uso y/o exportación de criptografía fuerte, ya había afirmado una vez que no debilitaría intencionalmente los estándares de cifrado (véase la RFC 1984; sobre la historia de las declaraciones políticas del IETF, véase la **presentación** de Brian Carpenter, ex-presidente del IAB y del IETF, Universidad de Auckland).

DNS-SD: Un Sistema de Nombres de Dominio (DNS) local

El Grupo de Trabajo sobre el descubrimiento de servicios de DNS (cuyos estatutos fueron aprobados el 25 de octubre) tuvo su primera reunión, y se abocó directamente a la pregunta acerca de si debería solicitar un TLD especial a ICANN para el enlace local que se utilizará como "raíz" para el descubrimiento de servicios locales.

Ralph Droms, co-presidente del nuevo GT, dijo que se habían mantenido conversaciones entre el IAB y ICANN acerca de una posible **asignación de un TLD**. La pregunta era si el IETF debería enviar una solicitud a ICANN, o si debería decirle simplemente qué TLD había elegido para el enlace local. Como ICANN está asignando más de mil nuevos TLDs, declaró Droms, se conversó acerca de la posibilidad de adoptar un TLD dedicado sin dominios registrados. El presidente del GT sobre el DNS, Peter Koch (Denic), señaló que en lugar de tratar con ICANN acerca del otorgamiento de un TLD de este tipo y de cómo asignarle uno al IETF, una opción sencilla sería tener un subdominio bajo .arpa.

El IAB todavía no terminó de discutir el tema, declaró el miembro de este consejo Marc Blanchet. Una pregunta que fue motivo de debate en la sesión fue por qué Droms había incluido "legible para humanos" como característica del futuro TLD local. Dado que había muchos no angloparlantes, este requisito era innecesario, dijo Geoff Huston (APNIC). Dave Thaler (Microsoft) y otros afirmaron que la decisión de utilizar una etiqueta en este momento no debería excluir el agregado de otros TLDs para el enlace local. Por ejemplo, los subdominios serían una manera de ampliar el espacio.

Se espera que el DNS-SD permita "el descubrimiento de servicios más allá del enlace local, utilizando distintas técnicas ad hoc". Este mecanismo superará las limitaciones de una red de enlace único, y será escalado a redes multienlace. El inicio del trabajo de este grupo no se produjo sin conflicto, ya que existe preocupación acerca de la posible "fuga" de direcciones del enlace local a la red externa.

Las redes domésticas y de pequeñas empresas, así como las de universidades y empresas más grandes, deberían poder utilizar el descubrimiento de servicios de DNS locales. Según **el documento de requisitos** presentado en Vancouver por Stuart Cheshire, Apple y Kerry Lynn (un consultor), para las redes más pequeñas la configuración cero es un requisito. Para las versiones más grandes, las opciones para configurar, por ejemplo, varios ámbitos de descubrimiento para un solo departamento y para la red de la universidad en su totalidad también constituyen un requisito. Apple ha estado presionando para que el DNS-SD mejore su servicio "Bonjour", y quiere que lo escale a una variedad de "cientos de miles de dispositivos habilitados de DNS-SD/mDNS en un entorno determinado".

En la lista de aspiraciones del nuevo GT están la implementación gradual y la ausencia de conflictos con el descubrimiento de servicios ya existente (a través de mDNS). Además, los usuarios no deberían encontrar diferencias entre la resolución local y la global.

Ciertamente, la controversia sobre la propuesta que se está considerando está lejos de haberse resuelto completamente. En un **documento presentado** justo antes del IETF 88, Andrew Sullivan (Dyn DNS) propuso un "perfil de máxima interoperatividad" (MI), que minimizará posibles conflictos resultantes del uso paralelo de DNSSD en entornos DNS y mDNS (DNS multipunto). Las tres reglas principales introducidas por el perfil MI de Sullivan serían las siguientes:

1. si la etiqueta está hecha enteramente de puntos de código de Letra-Dígito-Guión (LDH por sus siglas en inglés), entonces la etiqueta DEBE ser una etiqueta LDH;

2. todos los puntos de código de LDH DEBEN ser convertidos a minúsculas;

3. si la etiqueta contiene cualquier otro punto de código, entonces esta DEBE ser una etiqueta-U bien formada.

Sullivan aconsejó no implementar algunas de las recomendaciones sobre el mDNS (RFC 6763) que podrían crear conflictos con las etiquetas IDNA2008. Por ejemplo, "los espacios y la mayor parte de los signos de puntuación no se permiten ni en las etiquetas-U ni en las etiquetas LDH". Además, como las bibliotecas tratarían "cualquier etiqueta codificada con caracteres Unicode como etiqueta-U propuesta e intentarían realizar la resolución en forma de etiqueta-A, es probable que el consejo de almacenar y transmitir etiquetas como UTF-8 en el DNS tropiece con problemas, y NO SE RECOMIENDA". Los distintos sistemas de reglas de mDNS y DNS tienen que ser regidos por un conjunto común de reglas. Es probable que la fuga de datos desde la red interna a la externa continúe.

BoF sobre el uso de GeoNetwork

Un BoF sobre el uso de GeoNetwork, que había sido impulsado por un proyecto de la UE (Mobile 2.0) acerca del enrutamiento de datos sobre tránsito y automóviles, no logró suficiente apoyo en Vancouver. Los temas abiertos que el equipo del proyecto de la UE quería tratar relacionados con la estandarización eran: geo-direccionamiento en la red cableada, geo-enrutamiento, intercambio de información sobre el área de destino y búsqueda y traducción del área de destino a una dirección de IP.

Después de la sesión, el director del área llegó a la conclusión de que para crear un grupo de trabajo haría falta un esfuerzo mucho mayor. El problema descrito se vincula con la distribución de información desde un enrutador de acceso a todos los nodos de destino en un área (por ejemplo, automóviles), y la llamada de vuelta desde estos al nodo local. Se mencionaron posibles problemas vinculados con la privacidad, pero no se trataron.

Novedades del IETF

Ahora el IETF tiene una Política anti-acoso, y nombró a Linda Klieforth (ISOC) como procuradora temporaria. La política no fue muy debatida, pero parece ser una expresión más de la evolución del IETF hacia una "organización" que siente que está mucho más expuesta al escrutinio público de lo que lo estaba antes. ISOC está preparando un video promocional del IETF que será utilizado para presentar la organización a otras comunidades (IGF, entre otras).

En este enlace puede encontrarse información acerca del trabajo en curso sobre el formato RFC. Un pedido de licencia "Creative Commons" para el Tao del IETF no podría resolverse sin cambiar la política de licencias de la Fundación del IETF. Se están realizando pequeñas modificaciones.

Varios documentos preliminares sobre el proceso de estandarización del IETF están siendo considerados en este momento:

1. sobre la aclaración de "estándar propuesto"

2. sobre el consenso aproximado y el voto sonoro

3. sobre las directrices para la conducta de los participantes en el IETF (que harán obsoleta la RFC 3184)

La próxima reunión se realizará en Londres del 2 al 7 de marzo de 2014.