BARCELONA – Taller sobre las DNSSEC (3 de 3)
Miércoles, 24 de octubre de 2018 – 13:30 a 15:00 CEST
ICANN63 | Barcelona, España

RUSS MUNDY: A ver si la gente del taller del DNSSEC se junta, así podemos comenzar rápido.

Creo que lo primero que tenemos que hacer es decir muchas gracias a nuestros patrocinadores del almuerzo. Espero que todos hayan comido bien. A mí me gustó. Afilias es el sponsor junto .CA y SIDN.

JACQUES LATOUR: Bienvenidos. Vamos a tener un panel en la próxima hora aproximadamente, hora y media. Es una presentación y panel de discusión. Primero tenemos a Wes Hardaker quien va a hacer la presentación de Viktor.

WES HARDAKER: Es una combinación de ambas. La mayor parte del material viene de Viktor Dukhovni. Soy Wes Hardaker, de la USC-ISI. DANE, SMTP y estadísticas de DNSSEC. De esto va a tratar esta conferencia. Les voy a dar un poco de contexto de cómo funciona el SMTP con y sin DANE, y por qué es mejor. Después vamos a mirar algunas implementaciones y estadísticas que Viktor y yo armamos juntos. No ayuda mirar mis diapositivas. ¿Podemos achicar un poco el tamaño, por favor?

Necesito poder ver el diagrama. Más pequeño, por favor. No tienen que leer las palabras.

Cuando ustedes envían un email y cuando lo leen, seguramente saben que están usando cosas seguras. La laptop envía cosas a un ISP y el ISP lo envía después. Necesitas un username y password, que van sobre SMTP protegido con TLS a tu ISP. Por otro lado tenemos IMAP. IMAP también necesita TLS y se conecta con el ISP para recolectar el mail.

El problema es que entre estos dos puntos, como lo dice Viktor, ocurre un milagro. Entre los servidores todo está sin encriptar y sin autenticar, lo cual es fascinante. Si ustedes se fijan en esta arquitectura seguramente van a ver que si tuviesen una clase les habrían puesto una F.

Una solución a la seguridad de email es habilitar TLS, ver si se pueden conectar con otra persona usando TLS y después se van. Esto les ayuda a prevenir los ataques pero sigue siendo un problema de vulnerabilidad a los ataques BGP, DNS y STARTTLS. No funciona perfectamente pero es mejor que nada.

Este es un gráfico de Gmail. Es el crecimiento de STARTTLS, actualmente alrededor del 90%. Esto es del 11 de octubre. Es el crecimiento ingresante para gente que se conecta a ellos y lo envía menos encriptado, a pesar de que no está autenticado. Allí representa el 91% en la parte derecha del gráfico.

Mejores metas de seguridad SMTP más allá de encender TLS oportunistas. Hay que ser resistente contra los ataques. Hay que poder

lograrlo incluso en el primer contacto, soportar un entorno mixto, saber cuándo los otros están encriptando y también cuándo autenticar a cada uno de los pares.

SMTP no es como HTTPS. En HTTPS uno entra a un sitio y ahí tiene la opción cuando algo funciona bien o mal de continuar. El usuario tiene la capacidad de poder decir: “Sí, voy a seguir avanzando a pesar de que falle” o deshabilitarlo porque no le gusta el CA. Esto no funciona con el alojamiento de email porque no podemos hacer clic OK y seguir usando la conexión. No podemos evitar confiar en todos. Hay que confiar en todos los CA cada vez que se producen los certificados para poder luego interactuar con los demás.

Aquí entonces es donde el protocolo DANE aparece. En SMTP la presencia de un registro TLSA DANE indica que sí soporta TLS. Por tanto, se debe esperar una capacidad de STARTTLS. Si no lo logramos, alguien seguramente está tratando de que ustedes hagan algo encriptado cuando no deberían hacerlo. También se necesitan parámetros para el contacto. No vamos a entrar en eso ahora en detalle. No vamos a explicar cómo funcionan DANE y DNSSEC pero funcionan muy parecido a cómo funciona DNSSEC. No hay sido modificado. DANE también explica a los servidores SMTP finales qué certificados o autoridades de certificado deberían haberse usado para firmar el certificado que vas a recibir sobre SMTP.

Esta es la visión de alto nivel de DANE y cómo llegamos hasta aquí. Es la única solución para efectivamente proteger el mail incluso en el primer contacto. Hay que utilizar DNSSEC para poder hacerlo. Así es

como funciona DANE en la práctica. Si ustedes aplican DANE en sus servidores de correo, aquí tienen algunos tips para empezar rápidamente. Tengo 35 diapositivas. Hay unas 65 en realidad en total. Voy a hablar de 35. Todo el resto las utiliza Viktor. Están al final. Los aliento a que las vean pero este es el resumen general.

Primero, para coexistir con DANE hay que tener dominios firmados DNSSEC. Sin DANE, lo que sucede es que si un sitio no tiene DANE, si no está aplicando DANE, como muchos no lo están haciendo ahora, el DNSSEC tiene una denegación de existencia y entonces dice: “No hay que suponer que el sitio es seguro”. Esto funciona muy bien y DANE es el primer protocolo que requiere una denegación de existencia confiable. Seguramente ustedes escucharon del DNSSEC, que es lo que también lo hace posible. Esto le permite saber si se puede esperar o no que exista una conexión STARTTLS segura y que va a fallar si no lo logramos.

¿Qué sucede entonces cuando buscamos fallas? Al estar protegido con DNSSEC sabemos que tenemos que saltear esos hosts MX y no podemos conectarnos porque se espera que se inicie TLS y si no ocurre, sabemos que algo va mal y que no se debe continuar. Si todos los hosts MX son salteados por algún tipo de problema, por ejemplo no se logueó a tiempo, recuerden que el email es un protocolo diferido que va a estar en cola durante un tiempo. Puede incluso fallar hasta una semana.

Si ustedes van a adoptar DANE, lo más difícil es el DNSSEC. DANE no es tan difícil en sí y coordinar los records TLSA podría ser un poco más

difícil pero hay varias herramientas que lo facilitan. Una vez que ustedes aplican DNSSEC, aplicar DANE en el servidor de correo es bastante simple.

Para poder hacerlo para el DANE saliente, si ustedes tienen un agente de transferencia de mail como MTA, esto incluye Postfix, Exim y Cloudmark, van a poder simplemente habilitarlo y pueden tener un resolutor validante de DNSSEC cerca del MTA y tienen que poder llegar a la documentación de DANE sobre eso. Para un Postfix, por ejemplo, hay que tener un resolutor en la misma máquina y luego tienen que habilitar DANE con las opciones de configuración. No es tan complicado y lo pueden hacer incluso si la zona no está firmada. Se puede habilitar para la conexión saliente a pesar de que no tenemos DANE o DNSSEC habilitado para el correo entrante.

Para el path ingresante tienen que aplicar el servidor SMTP. Se necesita registros o records de MX firmados con DNSSEC. También hay que tener records TLSA firmados con DNSSEC para cada host MX y si está tercerizado… Hay mucha gente que terceriza su correo y mira el TLSA después. Ovh.net es uno de los más populares. Tienen que firmarlo también. Ambas zonas tienen que estar firmadas. Tanto ustedes como el proveedor en ese caso. Siempre tienen que garantizar que los certificados de llave siempre tengan una rotación.

Hay muchas herramientas de DANE que hacen que nos resulte más fácil. Pueden mirarlas después en esta presentación. Hash-slinger está escrito por Paul Wouters, que está sentado aquí en algún lugar de la sala. Hay muchas otras herramientas. Viktor tiene una llamada

danecheck. En las últimas diapositivas, si no tienen nada de esto instalado, Viktor tiene notas sobre cómo hacerlo simplemente con OpenSSL instalado directamente. Es un poquito más complicado porque se necesitan líneas de comando pero para nosotros es muchísimo más fácil. Aquí es donde yo digo que está mi servidor de correo, cuáles son las entradas de DNS para la zona. Se firma y listo.

Ahora les voy a hablar sobre la encuesta SMTP DANE de Viktor. Él le dedicó mucho esfuerzo a recolectar mucha información estadística, emails una vez por mes, listas de correo de aplicación de DNS, mucha información no solamente sobre DANE sino también sobre DNSSEC y el uso que tiene según todos los datos que él va recolectando. La gente le sigue pidiendo que ponga los datos en su sitio web porque quieren mirarlo con más regularidad y no solamente una vez al mes en mi antiguo email. Él puso estadísticas en stats.dnssec-tools.org. Espero poder hacer un poco más. No está perfecto todavía. No está completamente automatizado pero estamos cerca. Nuestra meta es tener estadísticas que se actualicen a diario sobre cómo su investigación ve DNSSEC y también cómo ve DANE.

Esto lo hicimos en conjunto. Lo seguimos mirando porque va a ir mejorando. stats.dnssec-tools.org. Aquí se reporta tanto DANE como DNSSEC. Así es como se ve el sitio web. Ven que hay un pequeño gráfico. Tenemos la implementación de DANE. Ahora seguramente va a haber cinco gráficos. Esto es un poco de los números. El resto de los datos que les voy a mostrar en la siguiente diapositiva está disponible allí también. Si quieren ver cómo es mañana, pueden ir en lugar de esperar a que Viktor lo actualice.

En la encuesta DNSSEC DANE, él monitorea dominios delegados de sufijos públicos y otros operadores, certificación de registros. Muestran dónde hay un problema con el servidor de correo y utiliza datos de la base de datos CZDS de ICANN, también de VeriSign y otros TLD abiertos como .FR, .SE, .EU, .NL. Ustedes pueden venir a hablarme y les voy a poner en contacto con él directamente. Su dirección de email está también allí. Hay muchas empresas de seguridad que han donado datos. Algunos de los datos en los gráficos vienen de un conjunto de datos que le permiten tener más información. Él está cubriendo 200 millones de candidatos. También hay records TLSA, Quad A, A y MX. También captura las cadenas de certificado de los hosts MX para ver qué es lo que coincide.

Vamos a ver ahora las estadísticas de la encuesta a la fecha de octubre de 2018. Hay 8.95 millones de dominios con registros validados DNSSEC. Cuando la gente viene y nos dice: “DNSSEC no está implementado”, eso no es cierto para todos lados. Hay mucha gente que ya lo está usando. Hay 323.000 dominios con DANE SMTP habilitado. Vamos a hablar un poco después de la discrepancia de esos números. Hay millones de usuarios. comcast.net, web.de, gmx.de. Comcast, de hecho, es uno de los primeros proveedores que aplicó DANE y que dio soporte. ¿No fue usted? No. Algunos de Comcast están aquí.

Hay 5.538 hosts DANE MX en 3.641 zonas. Vamos a hablar de eso en un momento. También hay 500 dominios con lookups de records de TLSA. Cuando tenemos una tecnología creciente también hay que mirar dónde están ocurriendo los problemas. Eso ocurre con cualquier

tecnología, ya sea de seguridad o no. La seguridad agrega un poco más de complejidad. Hay que ver cuáles son los casos de fracaso. También hay records de TLSA. Recuerden cuando yo dije: “Si ustedes publican un record para el servidor de mail, van a requerir que haya soporte de TLS”. Si el servidor de mail no hace TLS, no se puede tener el mail.

En términos de los TLD de primer nivel, estos son los dominios de DANE por mil. Felicitaciones a los Países Bajos, que tienen tres millones de dominios con DANE habilitado. .COM es el siguiente y luego .SE. En cuanto a la confiabilidad, los problemas ocurren en los dominios estacionados. En general, hay una falla en el funcionamiento de DNS ordinario. Luego hay un problema de denegación de existencia solamente en alrededor de 500 dominios. Vamos a ver en breve un gráfico con una cantidad muy baja de TLD que dejan de funcionar. El más alto es .ORG. Los TLD con muy bajo nivel de baja de funcionamiento son .BR que tiene 0.04%, lo cual realmente excelente porque también tienen uno de los conteos más altos. A pesar de que tienen un muy alto nivel de dominios… ¿Hay alguien aquí de .BR? Me encantaría hablar con ellos después porque el éxito es excelente. Viktor quiere saber cómo lo lograste. Quizá te puedo preguntar. ¿Tienen algún sistema de monitoreo habilitado?

FREDERICO NEVES: Sí, nosotros monitoreamos todas las delegaciones a diario y reportamos en forma mensual. Esa es la forma en la que tenemos estos números tan bajos.

WES HARDAKER: ¿Se contactan entonces con sus clientes registrados? .HK tiene 0.06% pero en realidad tienen muchísimos más dominios registrados. También hay unos TLD con high-breakage como .BANK. ¿Hay alguien de .BANK? No tienen que decirlo públicamente. Vengan a hablar conmigo porque a Viktor le va a encantar. .NRW y .RU de Rusia, también son bastante altos.

De nuevo, la lista está en el sitio web. Se dice que ya se actualiza diariamente. La cantidad de dominios que utilizan SMTP y DANE ha crecido drásticamente. Vamos a ver también la escala. La escala va desde 2016 a 2019. Son 325.000 dominios que utilizan DANE y SMTP. Recuerden que hay muchos que tercerizan los dominios. Si miramos el próximo gráfico que contiene la cantidad de zonas es mucho menor. Es de 3.600. Eso es porque hay muchos que están apuntando a nombres en este gráfico. La cantidad de servidores MX que están sirviendo DANE es muchísimo más pequeña porque también utiliza muchos servidores de correo.

De este gráfico estaba hablando. Ese es el que tiene 3.600. La lista de dominios DANE bien conocidos que lo usan está creciendo constantemente. Dimos esta charla en Puerto Rico y era la mitad de nombres. Hay algunos muy importantes. Obviamente, tendríamos que hablar con IETF, el proyecto TOR, Comcast, web.de, DNS-OARC. Todos estos son muy conocidos y tienen un trabajo fantástico. Son servidores de mail muy usados.

Hay muchísimos dominios cuasi DANE que es cuando la zona está efectivamente firmada pero lo que está apuntando el servidor no.

Google, ovh.net, la gente que terceriza el mail, a uno o a varios de esta lista. La zona original está firmada pero el lado del servidor de mail no y lamentablemente esto no funciona. Los números de la izquierda indican 1.400.000 registros MX apuntando a ovh.net pero ovh.net no está firmado.

La cosa con la que necesita ayuda Viktor es más listas de ccTLD con delegaciones firmadas. Cuantos más datos él pueda conseguir, más puede usar esas informaciones para actualizar los gráficos. Algunos de los saltos de los gráficos aparecen cuando él consigue sets de datos. Hay gente que habilita más y a veces esos gráficos marcan los saltos cuando él consigue información.

Obviamente, necesitamos más ayuda en arreglar las cosas cuando el DNS se rompe, cuando DANE se cae, que chequean las cosas y que chequeen la denegación de existencia. La gente no piensa que es importante pero con DANE lo es. Eso es lo que marca que se pueda hacer TLS. Por favor, permitan DANE saliente. Si no tienen un dominio firmado, si no firmaron su dominio personal, aun así pueden usar DANE para autenticar a otros servidores sin tener un dominio firmado. Luego, por supuesto, habiliten DNSSEC y DANE en los servidores MX de alojamiento, especialmente cuando se están alojando miles de dominios firmados con ovh.net o Google Mail.

Como decía antes, hay muchas diapositivas además de estas adicionales. No tengo tiempo para todas. Hay muchas con todo tipo de información interesante, con muchas otras cosas. Las avanzo y no las muestro. ¿Dejamos las preguntas para el final o ahora?

JACQUES LATOUR: Hacemos las preguntas ahora.

ORADOR DESCONOCIDO: Lo que yo tengo no es tanto una pregunta como un testimonio. Hace dos semanas me encontré con Viktor y hablando me dijo que tenía shells scripts. Necesité una hora para ponerlos en mi gestión. Si usamos Let'sEncrypt cada vez que refirmamos, se refirma la misma clave. Así no tienes que cambiar el TLS a menos que hagamos rotación de la llave, cosa que dejé para después. Ahora hay 43 servidores web firmados. Sabiendo que Viktor suele subestimar las dificultades, me sorprendió lo fácil que fue.

WES HARDAKER: Muy buen comentario. Voy a buscar una diapositiva. La segunda diapositiva del apéndice dice: "Lanzando las claves TLS". Hay maneras seguras de hacerlo y él sugiere un par de rutas distintas. Tiene razón. Cuando primero apareció DNSSEC y DANE no eran fáciles de usar pero hoy día es simplemente una cuestión de llamar a la persona adecuada y generar tres claves. Es mucho más fácil de usar.

ORADOR DESCONOCIDO: En tanto se tenga automatización es sorprendentemente fácil.

WES HARDAKER: Gracias por su comentario. ¿Alguna otra pregunta?

JACQUES LATOUR: Es más una observación. Algo que hacemos en .CA es enviar a Viktor la lista de nombres de dominio firmados cada dos semanas para que los incorpore a sus estadísticas.

WES HARDAKER: Él lo agradece mucho porque además de analizar las estadísticas se intenta evaluar el contexto. ¿Alguna otra pregunta?

JACQUES LATOUR: Gracias. Ahora Peter Koch de DENIC va a hablar del despliegue de DANE en Alemania, creo.

PETER KOCH: Sí. Gracias, Jacques. Tengo pocas diapositivas. Si me quedo sin tema voy a usar las diapositivas extra de Wes. Voy a dar algunos detalles con esas diapositivas de Wes si sobra tiempo. Primero voy a ajustar el zoom. Un poquito más alejado. Eso debería estar bien. Gracias.

Primero, hay un error en esta diapositiva. No debería decir “use”, uso. Fue un mal uso de la palabra “uso”. No se puede hablar de uso. No sé cuántas conexiones usan. Es un problema también que tiene Viktor y que Wes mencionó. Realmente no sabemos cuántos mails pasan por los canales seguros y cuál es el volumen de los distintos dominios. Somos un poco reacios a dar datos de zonas. Quizá no lo hicimos en tanto nivel de detalle como Viktor pero hicimos algo parecido.

Esto se ve muy gris. No sé si podemos ver la diferencia entre la izquierda y la derecha. Los que estuvieron hoy a la mañana recordarán que tenemos 16.2 millones de dominios y solo 100.000 están firmados. Hay solo 100.000 candidatos para DANE, que son los que están firmados. Eso es parte del contexto. Si los principales dominios de mail estuvieran debajo, eso sería importante. No sabemos mucho sobre eso. Wes mencionó que hay otros firmados. Si pudiéramos contar el número de mensajes, esto sería un aporte significativo al volumen de mails que se transporte de hecho con seguridad.

Esto se ve un poco mejor. De estos 100.000 nombres de dominio que están firmados con DNSSEC, 86.000 tienen al menos un registro MX en la zona raíz. Ese es el siguiente candidato posible de mail seguro con DANE. Creo que Viktor y Wes lo llamaron dominios cuasi DANE. Quedémonos aquí por el lado más tranquilo. El registro no solo tiene TLSA sino a la derecha el dominio del mail tiene que estar firmado. Son más o menos 86.000.

Por curiosidad entonces, aquí los targets… A Viktor le gusta hablar de los parámetros TLSA, el uso y distribución son de tipo 2 y tipo 3. Vamos a achicar esto un poquito porque se usa el algoritmo Hash que no es quizá tan importante. El interesante es el que está al comienzo. Alguien de alguna manera logró poner el certificado en el registro TLSA y llevó EDNS0 a sus extremos y el resto más o menos parece benigno. Como les decía, voy a aprovechar las diapositivas de Wes después para explicar un poco más los detalles.

El número de targets MX con TLSA es solo el 7%. No son muchos. Estuve analizando todos los dominios. Estos son todos los dominios, los 86.000. Independientemente de a dónde apunten estos registros, tanto dentro como fuera del espacio, solo el 7% tiene targets MX con registros TLSA. Es algo por supuesto a mejorar y aparecerá en la próxima diapositiva. Lo que significa que tenemos 1.300 targets MX que es el 7% que cubren 28.000 dominios. Sin embargo, y nuevamente esto se refiere a los dominios cuasi DANE, los siguientes dos targets MX que no tienen TLSA añadirían unos cuantos miles más. Alguien dijo que DANE es fácil. La dificultad quizá se subestime. Los que estuvieron aquí a la mañana recordarán que gran parte del despliegue del DNSSEC en el lado de la firma lo hacen los registradores que hacen full-service, que operan el DNSSEC en nombre de sus clientes y que apuntan a sus propias estructuras de mailing.

En este caso, operan y firman los dominios de los clientes y les apuntan a sus propios sistemas como los servidores de mail del registrador. Ese servidor, donde reside el mail, no está firmado. Dependiendo del tamaño del registrador y la complejidad del espacio de nombres y la complejidad de esa compañía en particular, puede ser un poco más difícil.

Viktor hizo un par de llamadas telefónicas, mandó un mail y se dio cuenta de que esto es un poquito más complicado. Estamos tratando de motivar a los registradores sugiriéndoles que esto podría ser una característica interesante. Hay muchas influencias no técnicas que quizá puedan inhibir el despliegue inmediato de estos otros 28.000. A veces no solo es cuestión técnica. A veces son cuestiones políticas. En

especial en las compañías más grandes los límites de responsabilidades son los que hacen que las cosas sean difíciles.

Voy a dejar esto porque me gustaría contestar a cosas que se dijeron antes. Parece ser bastante directo, conseguir que los números aumenten. No sabemos por supuesto cuántos mensajes salen de los dominios. No sabemos si son el mismo número de mensajes que de usuarios. Si DANE se despliega o si el registro TLSA se instala, eso parece ser fácil. El monitoreo y todo lo demás, como decía John, la encriptación, la firma, la refirma del certificado una y otra vez es lo que hay que hacer. Tener todas estas cosas en su lugar requiere un poquito más de esfuerzo. Ya existe bastante automatización pero, por supuesto, los errores dañan a la gente porque se corre el peligro de perder correos. Por eso la gente anda con cuidado.

Otra cosa que hay que entender es que si bien el despliegue se hace porque uno hizo bien las cosas y se hace el monitoreo adecuado, es comparativamente fácil hacer el debugging de los problemas. Viktor hizo un buen trabajo en la identificación de los problemas y ayudar a la gente a hacer el debugging de cuestiones muy específicas de DNSSEC.

Es interesante y sí, es fantástica la diversidad de software que existe en el campo. Lo que la gente ha logrado hacer con todo esto al mismo tiempo. Por ejemplo, en combinación con caching negativo, los registros TLSA no siguen el mismo patrón www.secondleveldomain.tlda o QuadA, que es una buena herramienta de debugging. Esto lo hemos hablado un par de veces en estos paneles ya. Hay cuestiones técnicas que requieren un experto. Quiero

agradecer a Viktor por esta actitud proactiva que él ha tenido. Esto es todo lo que tenía para decir respecto de cifras. No sé si podemos entrar en detalles más técnicos. Usaría sus diapositivas si el tiempo lo permite.

JACQUES LATOUR: Tenemos mucho tiempo. ¿Alguna pregunta para Peter?

RUSS MUNDY: Peter, vi algo hace un par de meses, unos seis meses quizá en los diarios, en los periódicos sobre una ley que se sancionó en Alemania respecto de la encriptación del mail. ¿Leí mal o está pasando algo en el espacio de las políticas, de la legislación, que ha hecho que se produjera un aumento en el uso?

PETER KOCH: No interpretó mal. Se aproxima bastante. No es una ley. Es el Instituto Federal de Seguridad de la Información. Ellos emiten directrices para la operación segura de los servidores de correo. Ellos estaban dirigiéndose a los ISP, a los operadores principalmente. Si bien esto no tiene una vinculación legal, no es obligatorio, hay una recomendación que tiene su peso. Como sabemos en estos círculos, el PSI, que es el acrónimo del Instituto Federal de Seguridad de la Información, defiende muchísimo lo que es DNSSEC y DANE. Incluyó este protocolo en su recomendación.

Nuevamente, no es vinculante pero hay mucha legislación de seguridad de TI en paralelo. Seguramente ustedes han escuchado de la directiva europea que después pasa a la ley nacional europea de los países europeos y todas estas cláusulas y probablemente me esté equivocando con la terminología pero habla de las medidas de tecnologías de avanzada. Puede uno interpretar por un lado o por el otro la recomendación pero esto sería considerado tecnología de punta aunque debo aclarar que esto no es una definición de características ni de mi parte ni de mi empleador. Por supuesto, usted tiene razón. Hay cosas que están pasando en el ámbito de la política que son importantes y que son congruentes con lo que estamos haciendo y con lo que han estado haciendo los Países Bajos también.

RUSS MUNDY: ¿Han podido detectar algún cambio en lo técnico, en el aspecto técnico por esta política?

PETER KOCH: No realmente. ¿Por qué? Cuando medimos aquí eso que les mostré hace un par de minutos, solo medimos el número de dominios firmados y targets MX. Eso representaría a todos. Los grandes ISP y todos, incluso aquel que tiene un negocio pequeño en el garaje o en el jardín. Lo que a todos nos gustaría tener, creo, es una indicación de cuántos correos fluyen por los canales encriptados y, mejor aún, por canales TLS con DANE seguro. No tenemos acceso a esa información. Por lo menos no es medible. Obviamente, las grandes ISP lo anuncian. Hace un par de años hubo iniciativa de hecho. Algunos proveedores de

correo alemanes se unieron. Hicieron algún tipo de grupo y negociaron canales encriptados entre ellos que por supuesto es un círculo cerrado interno que obviamente promueve las cosas.

Además, se encriptaron todas las sesiones IMAP entre ellos y forzaron de algún modo a los clientes a ir por estos canales encriptados pero no sabemos cuántos correos corren por ahí. Además, hay mucha atención de los medios especializados y de usuarios interesados. Gracias.

JACQUES LATOUR: Gracias, Peter. ¿Alguna pregunta? Jaap.

JAAP AKKERHUIS: Creo que esto se mencionó en otro workshop. En Holanda el gobierno tiene unas listas para la compra de servicios. Se establece qué es lo mínimo que se debe hacer. DANE está en esa lista explicativa. Hay una lista. Si uno tiene un contrato, tiene que ofrecer DANE automáticamente. Esa es la razón por la cual esto se hace así. Todos los países europeos pareciera que no tienen suficiente legislación porque lo único que hace es marcar el casillero y llamar al abogado. Ese es el ejercicio que hacen.

WES HARDAKER: Peter, algo que me parece que no mencionamos es que DANE es un mecanismo genérico para asegurar las conexiones TLS. Estamos hablando de SMTP porque ahí es donde empezó. ¿Ustedes han hecho alguna medición de servicios web? Los navegadores no tienen mucho

sentido, ¿pero hay algún otro protocolo basado en TLS que ustedes hayan analizado?

PETER KOCH: Francamente no, no lo hicimos por razones obvias. Hay poco por esperar de los navegadores. Sería una buena idea quizá hacer esto que están haciendo algunas personas por curiosidad, incluso quizá les sorprenda que los navegadores no adhieren a la información que está en el DNS. No lo analicé con más detalle.

WARREN KUMARI: Debo decir que hay un nuevo borrador en IETF que toma toda la información de DNS y la coloca en un certificado y luego toda la información está en ese certificado entonces. Eso permite que un servidor web se lo envíe a un browser. Eso quiere decir que el browser no tiene que ir al DANE en sí. No tiene que hacer lookups de DNS adicionales. Como usted dijo, se puede utilizar para otras cosas y para extensiones de TLS.

WES HARDAKER: ¿Sabe si ha habido algún compromiso de los navegadores para hacerlo?

WARREN KUMARI: Puede haberlo o no. No puedo comentar sobre eso.

JACQUES LATOUR: ¿Cómo se llama?

WARREN KUMARI: Una de las razones por las cuales varios navegadores no tienen DANE es que requiere hacer muchos otros lookups de DNS. Algunos fallan porque algunos lookups de DNS fallan siempre. Lo que hace esto es que toma toda la información de DNSSEC y la coloca en una extensión en el certificado. De ese modo, cuando uno recibe el certificado que tiene toda la información de DANE y el navegador o cualquier otra aplicación no tiene que ir a los lookups de DNS en sí y la persona que está sentada junto a mí está muy involucrada en esto.

PAUL WOUTERS: Hola. Soy Paul. Usted tiene razón. Había una forma antigua de hacerlo que era colocarlo en el certificado pero eso no avanzó. Ahora se coloca en una extensión TLS. No es un certificado. Es importante porque está separado de la PKI. Algunos navegadores querían implementarlo pero hay una gran discusión en cuanto a cómo hacemos avanzar este documento y por qué tomo nueve meses tener un borrador nuevo. Hay muchos mensajes en una lista de correo. La gente está interesada en este trabajo que está ocurriendo pero en una dos semanas seguramente vamos a poder avanzar un poco más.

PETER KOCH: No le voy a pedir a la audiencia que me hable del panel. Esto está vinculado con DANE pero también con la seguridad de transporte del email. Si recuerdo bien, hay trabajo que se está haciendo sobre la

seguridad del transporte para SMTP. Si mi memoria funciona bien, hay un proyecto adicional que tiene que ver con indicar el transporte en el mensaje o al receptor del mensaje. Eso podría ayudar al menos al usuario ocasional a encontrar que el correo se transportó con seguridad o no. Quizá alguien pueda explicar eso. Yo puedo ayudar a los usuarios a entender de qué se trata, si es que son o no parte de esto, quizá hay que hablar con el ISP en una forma parecida.

WES HARDAKER: Algunos tienen el equivalente a hacer un pinning que no ayuda mucho, ciertamente en el primer uso. Si alguien puede insertar records MX, pueden dirigir tu mail a cualquier parte. Pueden tener cache poisoning. Si no hay DNSSEC habilitado, pueden cambiar los registros MX a una persona que le envió un mail. De todos modos, se lo pueden enviar a ustedes. Van a tener una copia y van a saber que lo van a recibir. Cuando Viktor y yo trabajamos en el borrador SMTP hay que empezar en DNS. Al tener el record de DANE en DNS, se evita que todo lo que está en el medio y el resto de las soluciones no dejen de funcionar.

JACQUES LATOUR: Tengo una observación. Los navegadores no hacen pinning de certificado con nombres porque no hay ningún record de DANE para testearlo. Si nosotros agregamos más registros, vamos a tener que estar seguros de que funcionen. Si firmamos más dominios y tenemos TLSA disponible en el sitio web, a pesar de que el browser no lo haga, debemos habilitarlo. Ahora no está habilitado.

WES HARDAKER: Creo que lo que usted dice es que si publicamos los registros de TLS para los navegadores, ahí se podría indicar. Cuando hay suficiente aplicación, lo van a habilitar pero yo no creo que eso sea cierto. Nosotros pusimos DANE en Bloodhound. Hay un navegador que soporta DANE.

WARREN KUMARI: Si suficiente gente publica records de DANE, hay una posibilidad razonable de que los records TLSA quieran hacerlo también. Es poco probable que los navegadores quieran utilizar DNSSEC DANE. Hay mucha latencia y hay ciertos usuarios que no van a poder tener records DNSSEC firmados. Los records TLSA o DANE pueden molestar en el registro DNSSEC.

WES HARDAKER: Hubo una discusión respecto de que cuando uno muestra la página cuando DANE falla…

WARREN KUMARI: Esa es mi idea. Ellos tienen razón. Para cuando esté todo listo, las cookies se envían al sitio inadecuado. En ese caso, no importa porque lo pueden emular de todos modos. Tienen razón. Yo estaba equivocado.

JACQUES LATOUR: Muy bien. ¿Hay alguna otra pregunta? La siguiente presentación de Wes es Acelerar el Resolutor DNS con la Raíz Local.

WES HARDAKER: Mi primera súplica sería que todos deberían trabajar en presentaciones para el taller del DNSSEC, así no tendrían que escucharme a mí tres veces en un día. Aquí hubo cambios de último minuto. Yo estoy remplazando a alguien simplemente.

Hace un año hablé sobre un proyecto mío que se llamaba LocalRoot. Todo el propósito de LocalRoot era mostrar una actualización de cosas que pasaron. No voy a necesitar 20 minutos. Esta es una captura de pantalla del sitio web. Es localroot.isi.edu, si quieren entrar al sitio ahora mismo.

El objetivo de LocalRoot es hacer dos cosas. Tiene que hacer pre-caching de records DNS. Originalmente, eran solamente datos de la zona raíz. Ahora hay tres zonas. Me voy a referir a eso en un momento. Quería que fuera muy fácil de implementar. Tiene que ser fácil porque simplemente hay que copiar y pegar. Soporta RFC7706.

ORADOR DESCONOCIDO: ¿Es una característica?

WES HARDAKER: Sí. ¿Por qué queremos usar LocalRoot? Pasó ya un año de esto. Lo que hace LocalRoot es permitirles tener una copia de toda la zona raíz pre-cacheada. Esto es bastante fácil de hacer hoy. Aquí les da

notificaciones. Les asegura que la conexión entre ustedes y el servidor es segura. También allí hay beneficios, especialmente va a tener aceleraciones locales. Al tener la raíz en el resolutor local, si uno no hace preguntas y ya uno sabe la respuesta, esto va a acelerar la resolución. Es cierto también para las zonas de records donde hay records DNS, etc. Evita que deje de funcionar. Si hay una copia de la zona raíz y uno la transporta al proveedor cuando no está funcionando, todavía puede haber una copia local. Es poco probable que se produzca un corte en la zona raíz. Una de mis metas es soportar otras zonas también. Hay tres ahora.

Es protección de la privacidad. Yo hice una presentación anteriormente, no recuerdo si la hice en ICANN, donde muestro que incluso si ustedes hacen minimización de queries y utilizan TLS, solamente al hacer preguntas están liberando datos. Si ustedes van y piden los records NS para .RU, sé que estamos hablando de Rusia. Si están hablando de .BANK, sé que están haciendo banca. La mejor forma de proteger la privacidad es no hacer preguntas. Si ustedes tienen todas las respuestas pre-cacheadas es mucho más privado.

La RFC7706, su meta principal es brindar respuestas negativas más rápidas a los resolutores stub que tienen consultas basura y hay que evitar que estas consultas sean visibles en la red. Antes había una línea naranja en uno de los gráficos que les mostré. Allí veíamos toda la basura aleatoria que entra.

La realidad es que la mayoría de las consultas a la raíz no existen, como les mostré en el gráfico antes. Las respuestas negativas son

cacheadas por un tiempo corto. Si una hace la misma pregunta todo el tiempo, no hay datos reales de ese cache. Esto puede pasar si ustedes están en un link más lento. Si están en una parte alejada del mundo, yo no sé cuál es la velocidad de Internet que tengo en casa pero no es estelar.

El tráfico de DNS es observable en caminos de terceros. Esto es bajo el 7706. De nuevo, 7706 significa que no hay preguntas para revertir la red. Aquí llegamos a la parte de la actualización. Lo más importante es que se cambió el nombre de las claves TSIG que estaban vinculadas a mi servidor. Lamentablemente, TSIG tenía que ser único y no puede cambiar pero yo lo cambié. Si ustedes están usando LocalRoot van a tener que tener una nueva copia de la configuración. Esta es la última vez que lo haga. Les garantizo que va a ser una única vez y que no habrá que hacerlo otra vez.

Ahora es posible borrar los nuevos servidores. ¿Cómo puedo borrar? Eso es lo que me preguntan. Hay una nueva preferencia de notificación de cuenta de email. Ahí se pueden recibir actualizaciones, se pueden recibir partes de información. Yo todavía no mandé nada pero lo voy a hacer pronto. Hay una gran cantidad de interfaces de usuario. Algo que debo mencionar es que el taller de DNSSEC antes de que existiera DNSSEC todo este proyecto no podría haber ocurrido. Esto es lo que les permite poder confiar en las fuentes de datos.

También soportamos nuevas zonas: .arpa y rootservers.net, que también están allí ahora presentes. Muchas mejoras a las pantallas de los servidores. Desde el punto de vista del debugging son muy útiles.

Se muestra también el último horario de transferencia. Aquí hay una captura de pantalla donde muestra que ese servidor está activo, que está habilitado, que tiene una configuración. Hay un botón a la derecha. A la izquierda se muestra el último horario en el que ustedes tomaron algo de la zona.

Hay una pantalla de generación de configuración mucho mejor. Ahora la pantalla es dinámica. Se puede tener una configuración total. Se puede tener una con configuración parcial. En ese caso, hay que insertarle coses. Automáticamente incluye los espacios de dirección privada si se trata de un resolutor que sirve a direcciones 10.loquesea o 192.loquesea. Se pueden poner estas configuraciones para permitir el servicio.

Por supuesto, una de las cosas en las que me doy cuenta que estaba defaulteando sobre dónde guardar los archivos de la zona raíz y dónde iban a estar los esclavos, eso no existía antes. Ustedes ahora pueden especificar dónde poner los archivos. Este es el principio de cosas que yo realmente quiero hacer. Seguramente voy a tener una aplicación muy pronto para que algunos de mis estudiantes u otros me ayuden a hacer cosas interesantes como mejorar la infraestructura. Ahora hay un servidor de DNS que va a transferir la zona. De hecho, esto va a provenir de la versión de TSIG que solamente va a funcionar con el mío. No soporta todavía IPv6. Sé que la gente lo quiere. Seguramente va a venir pronto. Quiero poder mandar notificaciones de email cuando el TSIG no funciona bien para recibir una nota donde dice si lo deshabilitó o si hay algo que está mal. Lo mismo ocurre con las conexiones TSIG, si es que hay algo que esté mal con la llave, etc.

También hay que soportar Unbound y otras configuraciones de resolutor. Seguramente esto va a ser bastante fácil. Otras fuentes de datos de DNS, este seguramente va a ser mi proyecto más grande, que es el que más trabajo va a requerir que es poder tener una lista seleccionable. Si ustedes utilizan un TLD para el cual nosotros tenemos datos, hay que ir y traerlos. Seguramente no les puedo traer el .COM. La máquina seguramente no tiene la memoria porque los de .COM son muy impresionantes, pero hay muchos TLD que son más pequeños y la información solamente hay que pedirla. Hay muchos lugares en los que yo sé que puedo tener dominios importantes. He hablado con algunos vendors que quieren explorar este territorio también. Esto va a venir en algún punto. Estoy deseando conseguir esa pieza. Por supuesto, quisiera publicar todo este código. No hay ninguna razón por la cual yo no lo deba hacer.

ORADOR DESCONOCIDO: ¿Alguna pregunta? Si quieren entrar a localroot.isi.edu, si administran un resolutor, es muy bueno cortar y pegar y generar servidores y conseguir la configuración y hacer muchas otras cosas mediante cortar y pegar. ¿Alguna pregunta?

JACQUES LATOUR: Jaap, la primera.

JAAP AKKERHUIS: Recuerdo que había que hacer algo. Este mecanismo en Unbound en producción no está en este momento activado. Es una manera distinta

de hacer las cosas. Además, hace un tiempo que viene funcionando. Resolvió el problema. Si se conecta a través de un satélite y algo le pasa [inaudible], no se puede resolver localmente ya cuando la información expira sino a través de la cache local. Eso ayuda, al menos para que la comunicación local sepa qué hacer en la conexión. Eso ha funcionado con este tipo de sistemas.

WES HARDAKER: Es muy importante esto. Este fue uno de los propósitos principales, en especial de la investigación de latencia, el uso de satélites, una vez que se perdió hace mucho ruido. No estamos compitiendo tanto, tiene razón. Usted habla del proyecto de la ICANN que también lo hace para BIND. Ambos servidores de nombres tienen la capacidad de pull. Esperamos hacer más, más habilitación y también notificación para que el servidor tenga notificación e ir a buscar al servidor de raíz X ahora o el resto de los TLD. Lo que puedan hacer eventualmente e ir a buscar ese abordaje de ir a buscar periódicamente.

ABDALMONEM GALILA: ¿Imaginan cómo sería si la zona del servidor local se firmara con DNSSEC? ¿Cuál es la cadena de confianza?

WES HARDAKER: Usted hace pull de la zona raíz de IANA real con sus claves y su confianza. No cambia nada. El DNSSEC funciona igual. Se pone en el archivo de zona y es como una copia. Es como si hubiera hecho un query temprano de la raíz y ya recordara todas las respuestas. No hay

diferencia de seguridad. Es el mismo conjunto de claves. No se está haciendo refirma. La misma confianza.

ABDALMONEM GALILA: Creo que es una buena idea para blockchain, usar DNS como servicio de blockchain.

WES HARDAKER: Esto es una historia totalmente distinta. No está de hecho relacionado con blockchain.

WARREN KUMARI: Hay algo de trabajo en el IETF. No lo veo, Duane. Ahí está. Para que toda la información en la zona raíz se firme, incluyendo el registro glue y todo lo demás, ¿ustedes piensan que cuando esto pase, el registro TSIG estará o no?

WES HARDAKER: Va a importar menos. El TSIG se va a sentir mejor pero se va a sentir que importa menos. Tiene que ser el servidor correcto. Si está en el medio, con TSIG se consigue la zona más actualizada porque se confía a la persona que está del otro lado de la conexión. Se sigue trabajando.

DUANE WESSELS: Iba a preguntar lo siguiente. ¿Cómo alguien que recibe un archivo de zona de ustedes sabe que es el archivo correcto, que es la zona correcta y que ustedes no están manipulándola?

WES HARDAKER: Por DNSSEC. Lo que dije a mitad de la presentación no sería posible porque ustedes no confiarían en mí ni en que mi servidor les diera la información correcta porque tienen la zona raíz firmada por la KSK de la ICANN.

DUANE WESSELS: Quería ponerlo en un aprieto.

WES HARDAKER: Aun así, usted tiene que confiar. Yo le puedo dar un resumen. Eso funcionaría también aun cuando hay una cuestión de tiempo.

WARREN KUMARI: Alguien podría darle una zona antigua pero sería fácil saberlo porque al menos una vez por día se chequea. Esto se puede saber. Sé que podría ser equivocado.

WES HARDAKER: Para decirlo, hay que ir a chequear con otro, para asegurar.

WARREN KUMARI: Si es más de un día de antigüedad, es viejo.

WES HARDAKER: Cuando eso se hace, sí, la raíz local es uno de los lugares. LocalRoot es uno de los lugares donde chequear esto.

BRETT CARR: Brett, de Nominet. Acabo de iniciar sesión y me gusta que en su presentación usted lo dijo pero en el backup dice que el servidor soporta.

WES HARDAKER: Contacté a todos y hay muchos servidores que soportan AXFR y todos los que están listados me dieron permiso para dar la información. Es un sistema failsafe. No va a haber una transferencia de zona de alguien más.

ORADOR DESCONOCIDO: Muchas gracias por su trabajo, Wes. El RFC ya tiene un par de años y creo que es importante tener experiencia operativa aquí. Además, el escalamiento es algo interesante. En este momento es interesante ver que DNS es más tratada desde el contenido y no necesariamente por lo que es control central. Tengo dos preguntas. Usted sugirió extender esto más allá de la red. Por ejemplo, a los TLD. La pregunta sería cómo monitorearían la calidad. No tanto el contenido me preocupa sino la autenticidad y la integridad de los datos y la calidad de la entrega cuando un par de TLD pueden tener un lugar similar. Ese es un aspecto. Otro es que cambiaríamos al requerimiento y a los niveles de servicio de la respuesta de los paquetes del DNS al aprovisionamiento de la zona. ¿Eso significa que tenemos necesidad de una infraestructura totalmente distinta? Sé que la Universidad de California del Sur no va a ser el único lugar donde se hagan estas

cosas. Hay root servers. No sé dónde están pero tenemos que manejar la parte del sourcing. ¿Puede hablar más sobre eso?

WES HARDAKER: Puedo decir que esto no es un experimento porque es mucha infraestructura pero es tener un espacio, como usted decía. Si la zona raíz es el tema del que más habla la gente, ¿cómo podemos darles a todos los datos a través de otro mecanismo para que los tengan? Yo quería ir un paso más allá. No es solo la zona raíz. En todo el DNS tenemos lo que precisamente decíamos. Esto es pre-caching. Dar un conjunto de zonas finales con anticipación cambia las expectativas. Lo que yo hago no es en esta lista porque está más adelante es tener una suite de pruebas para comprobar que los resolutores funcionen bien pero eso ya lo tenemos. Tendría que tener ya la seguridad de que los resolutores funcionan bien. No es distinto en ese sentido. Con respecto a los datos, se tienen o no se tienen en la cache. La cuestión es si la cache es una zona esclava o si se está haciendo un pulling todo el tiempo. Esa es la pregunta.

JACQUES LATOUR: Tenemos dos. ¿Cuál va primero?

ORADOR DESCONOCIDO: ¿Por qué esto no se promociona LocalRoot para nuestros proveedores de servicio de Internet?

WES HARDAKER: Sí. Los ISP. Primero hay que probarlo con mucha gente para verificar su funcionamiento pero hasta ahora se ha usado en entornos pequeños y no hay motivo por el cual no pueda usarlo un ISP en una región completa.

DANIEL: No entiendo dónde está la fuente. Hacen un AXFR.

WES HARDAKER: ¿De dónde vienen los datos? Como decía el señor, hay una lista de servidores que la configuración de LocalRoot ofrece. Hay muchos servicios pero ofrecen AXFR como hace B, L, F. Hay varios. Ustedes pueden sacarlos directamente de ellos. Hay un servidor de DNS LocalRoot que permite hace transferencia segura con TSIG.

DANIEL: Y pasar esto por ejemplo a .COM. Se puede tener una subzona de .COM que solo tengan que firmar nuestro set.

WES HARDAKER: No hay razón por la cual no puedan hacerse subzonas. No una parte parcial de .COM. Tomémoslo como ejemplo. IETF.com no nos dejaría hacerlo. No se puede hacer todo .COM.

DANIEL: No todo .COM sino lo firmado.

WES HARDAKER: Yo estuve pensando en una herramienta que haga análisis artificial. No como lo hace LocalRoot sino para hacer pre-cache. Hacer un prompt todos los días, una vez por hora para que siempre esté en la cache. Eso se puede hacer. Habrá que hacer cierto aprendizaje de inteligencia artificial de la máquina primero.

DANIEL: Se puede animar a la gente a firmar el dominio porque se va a hacer pre-cache.

WARREN KUMARI: Algo relacionado. Algunos como Joey y yo hemos hablado de tener un servicio donde la gente pueda adherirse para intercambiar y dar sus archivos de zona en un lugar central, que sea un punto central de transferencia y usarlos como esclavos con una opción de cache flush, que la gente pueda solicitar este servicio.

WES HARDAKER: Le cuento que yo ya tengo el 90% de esa infraestructura lista para usted.

WARREN KUMARI: Seguimos hablando entonces.

JACQUES LATOUR: ¿Vamos bien de tiempo? ¿Alguna más?

ABDALMONEM GALILA: Corríjanme si me equivoco. Esto significa que cada vez que se intenta refirmar la zona el ISP tiene que tener una nueva versión del servidor raíz. La cache está desactualizada cada vez que pasa por el resolutor. Eso significa que el cliente caerá. Segundo, a lo mejor no confío en mi resolutor.

WES HARDAKER: Con respecto a su primer comentario, usted recibe una nueva copia de los datos de inmediato. Esa es una de las ventajas. Eso no importa tanto para la zona raíz porque no cambia tanto. Si se llega a otras zonas habrá actualizaciones recientes y ahí importa más. Para la zona raíz, muy pocos cambios se hacen. Cuando salieron los nuevos gTLD, cuando salió uno aparecía de inmediata pero nadie iba a buscar los nuevos de inmediato. Los nuevos gTLD llevan su tiempo para construirse, conseguir clientes y demás. Las firmas se reciben de inmediato. Todo eso, el archivo de zona, incluyendo las firmas. Se recibe una copia reciente de todo lo que ha pasado. Eso es lo que vimos en la investigación. La frecuencia de actualizaciones, no hay que ir constantemente a la raíz cada vez que se actualiza. Hay una notificación del DNS. El instante que se actualiza la zona se propaga y pasa por distintos sistemas pero son segunditos antes de que usted reciba la notificación. Es una investigación interesante que a lo mejor la gente puede hacer. No es un reloj sincronizado a cada hora específica del día sino cada vez que se hace una actualización.

JACQUES LATOUR: ¿Cómo hacen el roll en LocalRoot?

WES HARDAKER: En el resto de la ICANN esta tecnología se conoce como la raíz hiperlocal. Ese es el término que la junta está usando. Cuando hay una copia local de la zona raíz, nada de los datos entran en DITL. Esto a la gente le preocupa porque no hay visibilidad de los conjuntos de datos que se proveerán. Es como si todo el mundo manejara una zona raíz y DITL estaría muy vacío. Hay quienes consideran esto un problema y otros un beneficio.

JACQUES LATOUR: Supongo que la cuestión es tener el contenido lo antes posible. Eventualmente vamos a tener .CA dentro de Firefox o algo así.

WARREN KUMARI: ¿Es un compromiso?

JACQUES LATOUR: No.

WES HARDAKER: Yo hablé con alguien del .CA que estaba interesado en utilizar esto mismo. Esta es una de las razones por las cuales quiero publicar el código, para que tengan sus ISP locales. A pesar de que es grande, los

ISP locales lo pueden tener cacheado. Si hay un DDoS a nadie le importará. Deberíamos trabajar en eso.

AHMAD ALSADEH: Soy Ahmad Alsadeh. Soy fellow. Creo que la instancia de la raíz resolvería el problema de la raíz local. En lugar de tener una raíz local puedo hostear uno de los servidores raíz cerca de mi infraestructura o dentro de mi infraestructura en lugar de tener una raíz local. Si ustedes están de acuerdo conmigo, está bien. Si no están de acuerdo, ¿no le parece que su proyecto afectaría la cantidad de instancias del servidor raíz?

WES HARDAKER: Uno, sí, si hay una instancia de uno de los operadores raíz cerca de la caja seguramente no se necesita, si eso es lo que tratan de hacer. Sin embargo, nosotros nunca vamos a llegar al punto en el que haya hardware suficiente que se pueda enviar a todos los ISP del planeta. Eso no es algo que se pueda lograr. Esto permite que los ISP utilicen el hardware conocido. Ustedes simplemente van a instalar una copia localmente.

AHMAD ALSADEH: ¿Qué pasa con la ruta? ¿Se debe ir al servidor raíz y luego al servidor local de nuevo?

WES HARDAKER: Si usted tiene una instancia cerca, el software de servidor de nombre no usa siempre la misma caja mientras que si tienen LocalRoot porque lo está corriendo allí mismo nunca va a salir de esa caja. Si tiene una instancia, va a mandar cosas la mayor parte de las veces.

RUSS MUNDY: Tengo una pregunta para Wes. Cuando tengamos una mejor definición del tipo de estadísticas y de datos necesarios del servidor de raíz para ver si son datos DITL u otros, ¿esa es una forma de generar una hoja de ruta para incorporarlos a un subset de datos? Si la información está disponible y hay más instancias.

WES HARDAKER: Es una pregunta interesante. Yo no sabía que este tema iba a generar tantas preguntas. Les agradezco. No hay ninguna razón porque todos pueden contribuir DITL. No hay ninguna razón por la cual los operadores no puedan contribuir datos DITL y tampoco hay ninguna razón por la cual no se pueda producir el equivalente de RSSAC 002. Yo diría que definitivamente necesito implementar y no hay ninguna razón por la cual no lo pueda hacer.

WARREN KUMARI: ¿Usted confiaría en muchos datos DITL? Por ejemplo, si yo los posteo en mi instancia local.

WES HARDAKER: ¿No sería esto un proyecto de investigación interesante?

WARREN KUMARI: ¿Quiere fondos para investigar esto?

JACQUES LATOUR: ¿Hay alguna otra pregunta? Muy bien.

WES HARDAKER: Gracias a todos. Recuerden que tienen que escribir presentaciones así no me tienen que escuchar a mí.

RUSS MUNDY: Le agradecemos al panel de DANE y a toda la interacción y a las preguntas. Esta de hecho es una de las razones por las que nosotros tenemos estas sesiones, no solo para escuchar lo que está ocurriendo en la comunidad por parte de la gente que está haciendo el trabajo y que puede venir a hablar sobre lo que está haciendo sino también para tener retroalimentación e ideas nuevas y capacidades que provengan de la comunidad como un todo. Creo que esta fue una excelente sesión. Quizá tengamos que chequear el tiempo de lo que hizo Viktor para ver si coincide o no con el momento en que DANE presentó.

WES HARDAKER: Hay una persona que ya implementó LocalRoot. Lo tiene operando y está verificando y funcionando. Hay alguien en esta sala que ya lo hizo.

RUSS MUNDY: Muy bien. Fantástico. Gracias a todos los presentadores. Tenemos una situación interesante que aparece ahora y que es que nuestra sala de Adobe Connect está funcionando al parecer y la presentación no funciona. El último elemento de nuestra discusión hoy es una posibilidad de que la gente que está en la sala pueda pensar en lo que escuchó hoy, pensar en lo que le puede resultar interesante hacer y también dar una posibilidad de pensar en lo que ustedes quieran hablar la próxima vez porque nosotros tenemos estos talleres en cada una de las sesiones y esperamos poder tener otra en ICANN64. Por eso queremos que se vayan de aquí pensando no solamente en lo que quieren escuchar sino también en lo que quieran contar a los otros.

Gracias, Wes, por animar a los demás a presentar. Vamos a estar enviando probablemente a principios de año o quizá un poco antes de principios de año, vamos a enviar el pedido de participación. Lo enviamos a muchas listas de correo así que presten atención y piensen en qué querrían contar en la próxima reunión.

En términos de lo que cubrimos hoy, todos tienen su propio punto en el que les gusta estar en la estructura del DNS. Como mínimo piensen si tienen algún impacto en la zona, si es que son el titular de uno o cientos o miles de zonas para firmar. Trabajen con el registrador o el registratario. Ya hemos llegado al punto con DNSSEC y con la comunidad de los registratarios. Si no están usando DNSSEC, ustedes tienen registradores adicionales que pueden utilizar y que están haciendo DNSSEC. Es decir, se puede pasar los nombres de una zona a la otra o de un registro al otro y debo decir personalmente que eso lo

hice un par de veces simplemente porque el registrador con el que los tenía antes no hacía DNSSEC. Es algo que se puede hacer.

Utilizar las estadísticas. Trabajar con quienes hacen proyectos de investigación. Nosotros queremos involucrar a la mayor cantidad de personas posible. Tenemos varias empresas ahora. No es una cantidad enorme pero hay algunas empresas que tienen las firmas DNS en la zona publicada. Me alegra decir que parsons.com es uno de esos. Opera como una empresa con la zona firmada desde hace un tiempo.

De nuevo, al trabajar con los operadores no solo de los registradores sino también de los operadores de servidores de nombre, ahí estuvimos escuchando de muchos lugares donde se dan estos servicios. Participen de forma que ustedes puedan hacer uso y empiecen a pedirle a más gente que haga más cosas con DNS. Si ustedes son un proveedor de servicio o un ISP, tenemos un muy buen feedback hoy de otros ISP y pueden hacer más. Pueden alentar a la gente a que haga más.

Este grupo, esta comunidad de DNSSEC, ha sido excelente en los últimos 15-20 años. Se trata de compartir información y la gente está más que contenta por poder compartirla. Quédense en contacto. Si necesitan ayuda, contáctense entre ustedes. Con esto, creo que nos estamos acercando al final del tiempo que tenemos. Adelante, Matt.

[MATT]: Tengo una pregunta sobre la presentación. ¿Todas las presentaciones se van a cargar? Refresqué la página y no pude ver la presentación de Wes.

RUSS MUNDY: El taller de DNSSEC, por la estructura que tiene en ICANN, está dividido en tres partes. Parte 1, parte 2, parte 3. Patrik también nos dará unas diapositivas. Quizá la suya no esté cargada todavía pero las vamos a cargar después. Allí están. Muy bien. ¿Ha alguien que tenga algún comentario o pregunta? Sí, Jacques.

JACQUES LATOUR: Quisiera saber si hay temas ahora que la gente quisiera ver la próxima vez, ya que estamos en esto.

RUSS MUNDY: ¿Alguien quiere plantear un tema específico para que el comité de programas lo considere para la próxima vez?

ORADOR DESCONOCIDO: DNS utilizando deep blockchain.

RUSS MUNDY: Lo vamos a incluir en nuestra llamada a participación. Vamos a pensar cómo hacerlo. Otro más por aquí.

ORADOR DESCONOCIDO: El progreso del navegador en local y de las discusiones que hubo en la reunión de hoy.

WES HARDAKER: El mundo del navegador web y su interacción con DNSSEC y DANE.

RUSS MUNDY: ¿Hay alguna otra sugerencia?

JACQUES LATOUR: Yo quisiera hacer una pregunta. ¿Por qué no hay DNSSEC Quiz este año?

RUSS MUNDY: La realidad es que tenemos tanto material esta vez que elegimos no incluir el quiz, las preguntas.

JACQUES LATOUR: Si hay algún voluntario para hacer el próximo cuestionario, sería estupendo.

WES HARDAKER: Si yo hiciese el quiz, tendría que hablar una cuarta vez. Me dejo una pregunta para la próxima vez.

JACQUES LATOUR: Vamos a tener un cuestionario la próxima vez.

RUSS MUNDY: Muy bien. De nuevo, gracias a nuestros sponsors del almuerzo: Afilias, .CA y SIDN. Gracias a todos los presentadores. Esperamos ver a todos en el próximo taller. Tengan en cuenta el llamado a participación que les va a llegar pronto. Gracias.

[FIN DE LA TRANSCRIPCIÓN]