MONTREAL – DNSSEC para todos: guía para principiantes
Domingo, 3 de noviembre de 2019 – 17:00 a 18:30 EDT
ICANN66 | Montreal, Canadá

DAN YORK: Vamos a tener preguntas y repuestas en breve. Si quisieran acercarse porque estamos aquí en esta sala inmensa, por favor vengan hacia el frente. Tenemos un micrófono que vamos a poder ir circulando.

Mi nombre en Dan York, trabajo con la Sociedad de Internet y del tema del que queremos hablar hoy es, qué es DNSSEC, cuál es el objetivo que tiene y lo vamos a hacer a través de un par de cuestiones. Vamos a tener un par de skits, vamos a tratar de divertirnos un poquito.

Primero, ¿cuántos de ustedes aquí han implementado DNSSEC de alguna manera? Veo a algunos, muy bien. ¿Cuántos de ustedes no tienen ni idea de lo que es DNSSEC? Muy bien, veo aquí una súper posición con los que lo implementaron. Vamos a contarles la historia de los orígenes del DNSSEC en el año 500 Antes de Cristo.

Esta es Ugwina, ella vive de un lado del gran cañón en una cabaña y este es el que vive del otro lado. Les queda muy lejos ir y volver y por eso no pueden visitarse. En una de las visitas vieron que había humo que iba saliendo de esa caverna y se dieron cuenta que podían usar señales de humo, que las podían enviar para contarse más historias, hablar y obtener una mejor conversación.

Pero un día, en otra caverna cercana donde ahí está el señor Kaminski, empezó a mandar sus propias señales de humo. De repente Ugwina del

otro lado no podía saber cuál es la correcta, no sabe cuál es la señal que yo debería estar prestando atención, entonces empezó a tratar de identificar qué se puede hacer aquí, ¿cómo podemos hacer que funcione?

Entonces fueron a consultar a los sabios, al cavernícola Diffie que quizás podía tener una idea. Él fue corriendo a la cabina de Og y al volver vio esta pila de arena azul, un color muy raro que solamente existe en la caverna de Og. Sale, corre y lo tira al fuego. El fuego se convierte en un azul magnífico y de repente ahora Ugwina y Og pueden conversar porque ahora ella ya sabe cuál es el que proviene de Og y nadie más puede interferir porque saben de hecho que el humo azul es el que viene de Og y no de ningún otro.

Esto es lo que también sucede con DNSSEC, de algún modo divertido. Es asegurar que uno tenga la información correcta del emisor, es decir, es hacer algo específico de la información para que uno pueda ver cuál es la información única que proviene de esa persona.

Vamos a hablar un poquito más de la cuestión técnica, con un alto nivel así es como se expresa el DNS, terminamos con la raíz donde todos estos TLDs que están aquí, todas las distintas formas y tipos están ubicados y luego tenemos el segundo dominio. Un resolutor de DNS sabe cómo llegar a la raíz, sabe cómo pasar la jerarquía y cada nivel en ese caminito le dice al resolutor que vaya a hablar con alguien más.

DNS es una base de datos distribuida que va a ver cómo obtener la información de cada resolutor haciendo un caché a lo largo de todo el camino, pero no hay seguridad en el protocolo.Como en nuestra

historia alguien puede venir y espufiar o dar otras respuestas de otras maneras. Se puede envenenar el caché de esos resolutores porque una vez que almacenan la información, pueden quedar durante cierto período de tiempo.

¿Esta lista nuestra tropa? Vamos a hacer un acting. Les vamos a mostrar un poco cómo funciona esto, lo vamos a actuar. Vamos a ver a unos actores que van a actuar como un usurario que van a ir a buscar información sobre cómo conectarse con bigbank.com. Mientras se preparan aquí nuestros actores, muy bien, Wes va a ser nuestro usuario que va a hablar con el proveedor de servicios de internet, el resolutor y ese resolutor va a interactuar con nuestra jerarquía de DNS que se está reacomodando. ¿Pueden encender el micrófono por favor?

WES HARDAKER: Creo que quiero comprar un yate, siempre quise comprar un yate porque son unos barcos muy grandes que a mí me encantan. Voy a ir a ver qué pasa con el banco. El banco es www.bigbank.com para ver cuánto dinero tengo. ¿Puede darme por favor la dirección para www.bigbank.com?

WARREN KUMARI: Sí, es usted el cliente que a mí me gusta tener contento. Hola, raíz, aquí uno de mis usurarios quiere tener www.bigkank.com ¿me puede decir qué es?

FRED BEKER: Me encantaría decir que puedo, pero tengo un problema. En realidad, no, yo sé dónde encontrar .com usted preguntarle a .com.

WARREN KUMARI: Muy bien, lo voy a intentar. Hola, .com uno de mis usuarios quiere entrar a www.bigbank.com, ¿me dice dónde es?

ORADOR NO IDENTIFICADO: Bueno no conozco nada www., pero sé que bigbank.com está ahí.

WARREN KUMARI: Hola bigbank, ¿puede decirme dónde está www.bigbank.com?

RUSS MUNDY: Hola, señor ISP. Yo puedo decirle dónde está www.bigbank.com está en 2.2.2.3.

WARREN KUMARI: Muy bien, por fin tengo una respuesta. Hola señor usuario, www.bigbank.com está en 2.2.2.3, ¿puedo ir con usted en el yate?

WES HARDEKER: Bueno, mi yate no acepta repulsores, pero tengo mucho efectivo.

DAN YORK: Vamos a darles a todos un gran aplauso. Así es como opera el DNS, esto es lo que sucede todo el tiempo para todas las enormes cantidades de

consultas, pero vamos a hablar un poco sobre cómo podría funcionar esto. Vamos a generar otro intercambio, pero esta vez van a ver lo que sucede cuando un atacante está involucrado.

WES HARDAKER: Hoy es el día en el que me voy a comprar mi yate, tengo que entrar a bigbank.com para transferir mi dinero, ¿me puede decir dónde está? Porque me olvidé.

WARREN KUMARI: Bueno sí, yo también lo olvidé, voy a ir a averiguarlo. Hola, raíz, uno de mis usuarios quiere entrar a bigbank.com, ¿puede decirme dónde está?

FRED BAKER: Si supiera yo la respuesta. Sé dónde está .com, ¿le ayudaría?

WARREN KUMARI: Bueno sí. Hola .com, uno de mis usuarios quiere entrar a www.bigbank.com, ¿me puede decir dónde está?

ORADOR NO IDENTIDICADO: Bueno no sé sobre www., pero sé que bigbank.com está en 2.2.2.2.

WARREN KUMARI: Le voy a ir a preguntar.

ANDREW MCCONACHIE: Yo lo sé porque bigbank.com es 6.6.6.6.

WARREN KUMARI: Muy bien, no se preocupe. Hola, señor usuario.

WES HARDAKER: Creo que puedo ir a darle todo mi dinero a 6.6.6.6, gracias. ¿Dónde está mi barco?

ANDREW MCCONACHIE Gracias. Ja, ja, ja.

DAN YORK: Vamos a darle otro aplauso. Así puede quedar envenado DNS, quien pueda conseguir la respuesta al resolutor primero, gana. La velocidad, a ver quién puede llegar antes.

El doctor Malito puedo llegar antes de que pudiera dar el resolutor la respuesta. Ahora Warren, el que tiene el sombrero, el ISP va a quedarse con esa respuesta por un período de tiempo, entonces para todos los demás que preguntan dónde está www.bigbank.com van a continuar. Sí claro. Esa repuesta se va a repetir siendo errónea hasta el time out.

Esto que es el ataque de DNS, caché poisoning exacto. Lo que tenemos ahora, esto es DNS con DNSSEC agregamos a este concepto la firma digital, acá están nuestras tropas porque van a actuar nuevamente lo que pasa es que tienen claves y firmas guardadas dentro de DNS para poder verificar si esa información proviene de la fuente original.

Si es que realmente tiene que entregar la información para bigbank.com, entonces el resolutor para que todo funcione, sabe dónde está la clave de raíz, ¿cuántos de ustedes escucharon hablar de rollover o renovación de la clave raíz? Esto tiene que ver con verificar que haya una cadena de confianza desde la raíz de DNS en toda la cadena de los distintos servicios autoritativos que dan la información. Todo está vinculado para proteger la integridad de la información.

Lo vamos a hacer para que big bank acá sea el que da la información al ISP y no otra persona. Otra vez juntemos a la tropa como está acá y vamos a volver a actuar, pero esta vez con DNSSEC.

Tenemos que pasar por esto nuevamente, bien. ¿Qué hacemos acá? ¿La raíz está firmando? No le hubiera gustado a IANA que fuera tan fácil, entonces noten que la raíz firmó suyo el .com, big bank, todos firmaron, estamos bien.

WES HARDAKER: Supongamos que no pasó. Voy a comprarme otro yate. ¿Me puede contar dónde está bigbank.com y lo puede hacer bien?

WARREN KUMARI: Bien, vamos a probar. Vamos a preguntar a raíz. Hola raíz, uno de mis usuarios quiere ver dónde está www.bigbank.com, ¿me puedes contar?

FRED BAKER: No, no te digo, pero si te puedo decir donde averiguar .com, y .com puede decirte todo el resto, así que estoy firmado.

WARREN KUMARI: Vamos a verificar esa firma, me parece válido vamos a verificarlo con .com. Hola, .com uno de mis usuarios sigue queriendo comprar un yate, quiere saber dónde está www.bigbank.com.

ORADOR NO IDENTIFICADO: No lo sé, pero sí le puedo decir que bigbank.com es 2.2.2.2 y le firmó la repuesta.

WARREN KUMARI: Vamos a verificar la firma. Ah, me parece que está bien, voy a preguntar. Hola www.bigbank.com.

ANDREW MCCONACHIE: Hola.

WARREN KUMARI: Hola, ¿cómo estás?

ANDREW MCCONACHIE: 6.6.6.6.

WARREN KUMARI: ¿Dónde está la firma? No la veo. Bigbank.com, ¿me puedes contar dónde está www.bigbank.com?

RUSS MUNDY: Sí, sin duda. www.bigbank.com está en 2.2.2.3 y está firmada.

WARREN KUMARI: Vamos a verificar la firma con cuidado, sí parece que está bien. Bueno señor usuario, www.bigbank.com 2.2.2.3 lo validé, es confiable.

WES HARDAKER: Señor banco, ¿me puede transferir todos estos fondos a Nueva York para comprar el barco?

DAN YORK: Bien, Wes. Un aplauso para nuestros artistas. Así es como lo hacemos y de eso se trata DNSSEC, tener las firmas que verifican que no puede entrar otra persona al proceso, es todo lo que hace, una parte importante, verificar la integridad de la información que lo que entró al DNS es lo que salga del DNS no tiene que ver con confidencialidad, ni asegurar la información, puramente tiene que ver con la verificación de la información que sea exactamente lo que puso el usuario.

Para hablar un poco más vamos a traer a Russ Mundy que va a venir acá y le voy a devolver el dinero a Wes.

RUSS MUNDY: Muchas gracias, Dan. Gracias a todos que vinieron hoy en la tarde, qué luces brillantes. Vamos a hablar un poquito acá. Ah, bien para pasar las diapositivas, vamos a ver ejemplos de descripciones de la gente que tiene que pensar en el proceso de implementar DNSSEC. Parte del por

qué es porqué trabajamos con DNS, tenemos que ver desde la perspectiva de DNS, de la información cómo se puede complicar, especialmente si no tienen DNSSEC implementado.

Pero, ¿por qué la gente busca DNS? DNS no es tan interesante. Cuando la gente va a hacer cosas con DNS, quieren hacer cosas con aplicaciones que hace las consultas de DNS como vieron antes cuando estaba Wes tratando de transferir dinero, en ese momento era para robarlo.

Es importante para las aplicaciones que utilizan DNS, hacer lo que están haciendo, si no llegan al lugar correcto quien sabe qué va a pasar, entonces hemos tenido ejemplos múltiples en el mundo real de cosas de esta naturaleza. Y algunas de las cosas que se han identificado es que cualquier aplicación en internet hoy tienen una gran probabilidad de utilizar DNS por debajo y la mayor parte de las veces los usuarios de las aplicaciones no saben ni les importa que haya uso de DNS, pero es esencial para que funcionen las aplicaciones de manera adecuada.

Una de las cosas que he visto hace unos años, y volví, lo reevalué y lamentablemente no mantuve los detalles específicos hallados, pero había un profesor universitario que encontré en un curso de programación que requería que los alumnos escribieran un programa de hijack de DNS.

Y busqué en todos los requisitos del curso y no había nada que hablar de ética o de algo que no debieran hacer, les decían: “Vayan y secuestren el DNS”. O lo que llamamos hijack, la idea es tratar de evitar de que sucedan estos secuestros, no le he encontrado en los últimos

cinco años así que quizás ya no esté. Como decía Dan, lo importante es poder llegar al lugar correcto, y cuando llegamos al lugar correcto poder verificar que la información que se devuelve es correcta.

La criptografía de clave pública es integrada para que DNSSEC funcione su mecanismo técnico subyacente. En nuestros trabajos más antiguos las reuniones de ICANN ejecutaban secuestros reales, esto es una serie de diapositivas que nos dan una idea gráfica de lo que hemos visto en la actuación teatral.

Una de las razones por las cuales dejamos de hacerlo en la vida real es que en una de la reunión logramos en lugar de secuestrar el DNS en la sala en particular, la configuración de la red no era lo que se esperaba y secuestramos el DNS de toda la reunión de ICANN. Entonces imagínese lo que fue, lo que estaba pasando, ahora mostramos diapositivas.

Acá abajo a la izquierda está Joe que quiere ir al servidor de red que está ahí y fíjense de la imagen que manda, hay una consulta que va a servidor recursivo, que lo envía al servidor de nombres autoritativos asociado con la red, el servidor de red la manda al recursivo que a su vez le dice al usuario la repuesta. Esto es lo que vieron en el escenario recién.

Ahora después de eso se puede realizar la transacción. Cuando ponemos sitios reales, esta es una configuración específica con un sitio de internet para que la imagen visual del sitio aparezca con DNSSEC abajo, no hay una imagen estándar que lo muestre, esa es la idea, la idea era ponerlo en un sitio para que lo vieran.

Cuando van al mismo sitio cuando no están utilizando una validación de DNSSEC aparece un símbolo distinto, fíjense es una tilde cuando está y una advertencia triangular que dice que no está activado DNSSEC en el segundo caso. Cuando hacemos el mismo tipo de cosa como lo que mostramos teatralmente, se manda la consulta de Joe, pero acá está el Dr. Malito entonces la consulta va a otro lado y en el mundo real lo que pasa es que el Dr. Malito ve la consulta y responde, aunque la consulta continúa dando vueltas por la red, pero el usuario Joe va al sitio falso.

Y podemos ver que las otras consultas fueron a la red, volvieron, dieron una respuesta, pero Joe no recibió la respuesta porque al resolutor le mandó la primera respuesta y fue al lugar equivocado, no puede volver al lugar correcto salvo que utilice DNSSEC. Cuando sí la usa no permite la respuesta incorrecta evitando que llegue al resolutor y cuando recibe la respuesta correcta va al sitio correcto y lleva a cabo la transacción como corresponde.

Instrumentamos un sitio para mostrar lo que se puede hacer y específicamente fue construido de manera tal que hubiera una sección del mismo que muestre que hay un lugar donde puede haber un secuestro, y el secuestro propiamente dicho realizado contra un buscador de red que no estaba haciendo DNSSEC, insertamos información que era una historia inventada que decía que “Steve Crocker admitía que el DNSSEC no iba a resolver el hambre en el mundo”.

Era obviamente un tema humorístico de ilustración de lo que pasa, pero si se fijan que tenemos el triángulo amarillo arriba y abajo vemos .org, comparte el asesoramiento de DNSSEC a Comcast para los ISPs y en la parte superior esa es la historia más importante. Entonces insertamos parte de información en una página, aunque fuera la misma página del buscador era distinta la información y por supuesto, era falsa.

En una sola página va un servidor de nombre vacío sin información en caché, esto es CNN.com de hace seis o siete años y ahí hay aproximadamente 75 a 100 consultas y respuestas en una página, cualquiera puede estar secuestrada o una gran parte de las mismas.

¿Ha mejorado? No, en algunos casos sí, en otros no. Hay más consultas necesarias para llenar un sitio comercial que lo que había, pero esta instrumentación en particular muestra que ahora algunos tienen firma de DNSSEC, pero la cantidad que hace falta para llenar un sitio se duplicó en cuatro o cinco años aproximadamente. Lo básico que la gente a menudo le preocupa cuando habla de DNSSEC “ay dios mío, tenemos las claves criptográficas” ¿qué hace falta hacer para trabajar con las claves?

Es cierto, pero lo más importante son los datos de la zona de DNS. Tiene que tener por lo mismo la misma cantidad de cuidado sobre la precisión, la corrección de los datos que con las claves porque el hecho de tener DNSSEC asociado con cualquier zona es que el usuario que recibe la información sepa que la información de DNS es correcta, entonces si se ocupan más de las claves que de los datos en la zona y si

alguien quiere atacar la zona, van a atacar a la parte de su sistema que ingresa la información al sistema.

Y si firman esa información, quien la reciba va a decir: "Ah, tiene que ser buena, está firmada" pero si alguien tuvo éxito en el ataque, en el lado de suministro de la parte de DNS la información errónea, están peor en realidad que cuando no usaban DNSSEC porque ustedes como operadores están verificados a través de criptografía que la información está correcta y si no es correcta es culpa de ustedes por no manejar la información de manera correcta. Otro ejemplo de DNS sin DNSSEC.

Para datos de zona donde colocamos información dentro del servidor de nombres autoritativos, esa información ingresa, el servidor de nombres autoritativos está funcionando, recibe la solicitud de un servidor de nombres recursivos que también ha recibido el pedido del cliente y lo responde.

Se están incluyendo DNS en la operación de sus sistemas en lugar de tercerizarlo o de que haya un proveedor de registros que se lo brinde. Si DNS es importante para su función de lo que están operando, que hacen toda la operación dentro de la parte orgánica de su organización probablemente tengan en su personal gente que sepa del tema y van a querer hacer las actividades de DNSSEC como parte de la ampliación de lo que ya están haciendo para ejecutar DNS.

Las grandes actividades con DNS propio, especialmente cuando es crítico van a querer hacer la implementación interna y la operación también. Entonces si son un gran TLD, un registro o una empresa

hp.com que siempre ha sido un excelente ejemplo, verisign.com, su negocio está vinculado con DNS.

Entonces son organizaciones importantes desde la perspectiva del DNS así que van a hacer probablemente algo interno, sí la zona de DNS quizás no es tan importante para internet o para la viabilidad económica de la organización. En mi ejemplo acá sería que net.snmp.org que ese es un dominio mío, ¿no hace nada? Bueno lo transfiero.

Pero el hecho es que no es una operación crítica de DNS, no es crítica para el internet ni para la función del negocio y todos nosotros utilizamos DNS, tenemos que utilizar DNSSEC cuando podamos y lo importante es proteger los datos de la zona de DNS. Con todos los ejemplos de haber cargado la zona autoritativa y la solicitud de información y la repuesta, esta es una ilustración muy simple de los lugares que tienen que hacer unos pasitos más, dar algunos pasitos más.

Deben firmar los datos para la zona antes de que se cargue en el servidor autoritativo para esa zona, el servidor recursivo y la aplicación esperamos que ocurran en algún punto en el tiempo, pero el servidor recursivo en sí debe tener la clave de la zona raíz cuando se hace la consulta para que las respuestas cuando vuelvan puedan hacer la validación.

Para la mayor parte de los servidores de nombres de validación se puede encender simplemente encendiendo una configuración, eso es todo lo que se requiere.

En resumen, el concepto general de actividades que operan su propio DNS, el DNS es muy importante para ellos. Ellos van a querer hacer sus propias actividades de DNSSEC para asegurarse que está operando activamente, si una actividad tiene o a tercerizado su operación de DNS seguramente también van a necesitar tercerizar las actividades de DNSSEC.

En algunos casos es un poco más fácil, hay muchos proveedores de servicios externos de DNS, en el pasado no han ofrecido DNSSEC por eso quiero instar a quienes compran o tercerizan los proveedores de servicio de internet que no hacen DNSSEC, pídanles que lo hagan y no hay mucha gente que lo vaya a hacer, pero algunos lo hemos hecho.

Si no encuentran un servidor que lo haga, cambien a quien le dan ustedes el dinero para dar los servicios de DNS para que utilicen DNSSEC. Esta es una diapositiva de resumen, estas son las organizaciones patrocinadoras para estas actividades, vengan para acá arriba, el resto del tiempo tenemos a Willy que está abierto para discusiones, preguntas, respuestas. Les pedimos a todos que vengan y que realicen alguna pregunta.

DAN YORK: Muy bien, si quieren venir aquí y agarrar un micrófono. ¿Quién tiene preguntas? Alguien debe hacerlo. Andrew está aquí, Dr. Malito, ¿alguien tiene alguna pregunta para el Dr. Malito? Me imaginé que iban a empezar todos a hacer bromas y que podía ser doloroso.

ROCIO DE LA FUENTE: Muy bien, muchas gracias por esa representación y por la presentación también. Soy Rocío de la Fuente, soy fellow de ICANN66 y quisiera ver si entiendo correctamente, que la firma sigue la jerarquía del DNS, es decir, si el TLD no está firmado en mi registro de dominio, entonces quiero saber si tiene alguna forma de tener DNSSEC.

DAN YORK: ¿Alguno de ustedes quiere responder? La respuesta es la siguiente, se puede firmar el dominio, se puede hacer allí, pero no va a haber una cadena de confianza. Alguien que quiera validar el TLD no va a poder llegar hasta la raíz siguiendo toda la cadena, entonces sí, en general para que DNSSEC funcione el TLD tiene que estar firmado.

WES HARDAKER: Y también idealmente tiene que haber una protección desde la raíz hasta que sea firmado, la mayor parte de los TLDs hoy están firmados, van a haber gráficos que lo van a mostrar en algunos talleres, hay más de 10.000.000 de dominios firmados, pero hay que poder validar todo el árbol, es decir, que si se pueden validar hacía .com es mejor que nada porque big bank en sí no tiene ninguna conexión.

DAN YORK: El miércoles pueden venir al taller de DNSSEC, va a haber un par de cuadros que van a mostrar algunas áreas, produjimos algunos mapas que están en muchas partes y dependiendo… ¿Usted de que país es? De Argentina muy bien, .ar estoy verificando.

YAZID AKANHO: Hola, mi nombre es Yazid, soy de Benín, soy fellow de ICANN66. Gracias por la presentación y por esa especie de película que nos ayudó realmente a entender. Tengo dos preguntas, la primera, ¿por qué implementar DNSSEC? No sé muy bien que palabra usar, pero la implementación se hace sola digamos, es decir, ¿hay razones técnicas? ¿Hay razones políticas? ¿Por qué?

Segundo, me hablaron de un roadshow de DNSSEC que tiene un programa, ¿cuál es el próximo paso de un programa de roadshow de DNSSEC?

Y mi última pregunta, es tener una explicación sobre la infraestructura para generar las claves para DNSSEC. Me dijeron también que hay una infraestructura separada que debe ser mantenida, ¿puede explicar por favor un poquito?

DAN YORK: Sí. Implementación, roadshow, desafíos y de información sobre cómo hacer la firma, ¿está bien? Tome uno.

WARREN KUMARI: Acabo de hablar que .ar está firmado para la implementación sí, DNSSEC no se ha implementado en todo lo rápido que podría haberlo sido, pero algunas estadísticas porque estamos en Canadá en este momento, 13.3% de las solicitudes han sido validadas dentro de Canadá, 25% en Estados Unidos, 19% en Groenlandia, 14% en Rusia.

No está todo lo implementado, pero la implementación está aumentando y no la mayoría, pero una cantidad importante están siendo validados. Y la gran mayoría de los TLDs están firmados como parte del contrato de los nuevos gTLDs que están todos firmados, creo que la mayoría de los ccTLDs están firmados también.

WES HARDAKER: Si quieren ver un rastreo diario, mi colega Víctor que no me acordaba el nombre, tenemos un sitio web que actualizamos todos los días que se llama stats.dnssec-tools.org y les voy a mostrar, si miran el gráfico que continúa subiendo desde el año 2011. A veces hay subidas gigantes de one.com que es el proveedor y hubo muchas cosas firmadas bajo .dk.

Para poder tener la implementación necesitamos más, es decir, necesitamos enormes empresas que lo hagan por defecto porque la mayor parte de los dominios que están en uso en el mundo están operados por empresas que hacen hosting de DNS y tradicionalmente ha habido muchas subidas. En la República Checa también ha habido enormes incentivos para incentivar precisamente a la gente, es decir, que la registración se hace más barata y eso ha generado la firma de los códigos de país, por ejemplo.

DAN YORK: Russ.

RUSS MUNDY: Quisiera continuar con lo que se ha dicho aquí. Hay muchos incentivos que han sido utilizados por distintas organizaciones para alentar a la gente a que utilice DNSSEC, una de las áreas que ha ayudado enormemente es el hecho de que la mayor parte de los resolutores de DNS disponibles, la mayoría de ellos están utilizando validación de DNSSEC.

Algunos de nosotros hemos estado trabajando en algo que se ha estado haciendo hace mucho tiempo que es que queremos ver la validación aumentando hacia el final de la solicitud. Ahí es donde tenemos el ataque donde Steve Cropper, el secuestro de Steve Cropper estaba incluido, esa validación se hizo en el navegador en sí.

A medida de que ustedes tienen interacciones con la gente tengan en cuenta que cuánto más cerca ocurra la validación del DNS y de la información al usuario final más seguridad va a haber en el sistema en sí. Allí entran entonces la gente a pensar más allá, incluso del caching importante y de los resolutores públicos, piensen en las aplicaciones.

DAN YORK: Parte del desafío de implementación es lo que muestra esta imagen, en sí hay dos partes. Cada persona que firma o que tiene un dominio debe firmarlo, esta es una parte entonces o sea que es la parte de la firma. Parte puede ser automatizado si ustedes van a hablar con cualquiera de los proveedores de alojamiento de DNS, algunos lo hacen súper fácil, en algunos simplemente ustedes tienen que marcar una casilla y el dominio queda firmado.

Pero luego, la otra parte es que tienen que estar chequeando, validando como dijo Russ, a veces quitar un comentario o una línea de comentario en un archivo de configuración de repente empieza a validar. Parte de lo que sucedió durante mucho tiempo es que teníamos este problema del huevo y la gallina como decimos en Estados Unidos en términos de que algunos de los operadores de red, los ISPs como ha estado diciendo Warren que operan validación de DNSSEC.

Ellos estaban diciendo: "No vamos a encender la validación porque no hay suficientes dominios firmados" entonces los operadores decían: "Miren, no vamos a decir porque los dominios no están firmados". Y grandes proveedores de internet o de alojamiento decían: "No vamos a firmar los dominios porque no hay suficiente gente validada". Entonces se trataba de gente que hacía una pausa y decía esto, hoy parte de eso ha sido superado por lo que dijo Wes.

Hay verdaderas implementaciones, hay personas que están utilizando DNS público como el Google Public DNS, todos están haciendo validación de DNSSEC. Los grandes resolutores, los grandes ISPs lo están haciendo, Comcast está aquí en América del Norte con sus 20.000.000 de clientes, todos ellos tienen validación de DNS. Ese argumento de que se ha garantizado la implementación ya ha sido superado. Fred.

FRED BAKER: Quería hacerle una pregunta a Russ, ¿hay algún navegador específico que soporta validación de DNSSEC? Solamente tengo cuatro navegadores en mi laptop, ¿cuál debería usar?

RUSS MUNDY: Bueno, lamentablemente no hay un navegador disponible que tenga validación de DNSSEC incorporada. Nosotros tuvimos uno y lo suportamos, le dimos soporte durante un tiempo, pero ya no.

WARREN KUMARI: Creo que lo que ustedes están hablando es validación DANE. Todos los navegadores utilizan el sistema de resolutores, si la computadora hace validación de DNSSEC el navegador se basa en lo que hace el resolutor del sistema, es decir, que, si ustedes permiten validación de DNSSEC en cualquiera, ya sea el resolutor que utilice la computadora van a tener DNSSEC validándose gratis.

FRED BAKER: Usted me acaba de decir como usuario que en mi MAC o en mi máquina Windows o Linux tengo que ir a hacer algo.

WES HARDAKER: Es algo muy técnico, muy difícil de describir, pero hay elementos donde la validación puede ocurrir. Hoy las aplicaciones que incluyen lectores de Email, navegadores y todo lo que utiliza la red típicamente no hacen la validación por sí como el Skit, el usuario no chequeó esos certificados por sí mismos, sino que confió en el ISP… Soy una persona terrible,

entonces yo puse códigos de validación en el paquete net-snmp del cual estaba hablando Russ hace un momento.

Es decir, que tuvimos un código de validación en ese paquete para chequear la aplicación, muy pocas aplicaciones lo hacen. Una de las más grandes, de las motivaciones más grandes para que la gente lo firme es que se trata de una de las únicas formas o la mejor forma de asegurar el Email entre servidores. Esto está subiendo muy rápidamente, está aumentado no es todo el DNSSEC, sino que cuando miran el DANE que es la tecnología que firma las conversaciones de Email entre servidores eso está subiendo mucho y está cerca de la aplicación.

WARREN KUMARI: Fred, usted dijo como usuario que usted espera poder hacer algo, como usuario debe garantizar que los resolutores y los ISPs estén validando o que utilicen o elijan uno de los resolutores públicos 111199998888 porque todos hacen validaciones, si quiere protección de DNS puede utilizar los ISPs y si no utilice algunos de los otros.

También hay un sitio web internet.nl, allí es donde se chequea si los resolutores recurrentes utilizan la validación y ahí es donde se puede decir si el ISP la está haciendo o no.

DAN YORK: Fred, en cuanto a los navegadores vamos a dejarlo para el miércoles, pero hay cosas que están utilizando DNS sobre HTTPS, muchos de esos puntos finales están haciendo también validación de DNSSEC, es decir,

que el navegador posiblemente sí lo esté haciendo sí usa esa ruta, pero no hablemos de DoH ahora, vamos a la pregunta del usuario porque está esperando muy pacientemente.

YAZID AKANHO: Gracias por haber aclarado lo de los resolutores, la validación de resolutores y la firma de la zona que son dos cosas separadas y lo comprendo. Hace dos años en mi país, en Benín nos sorprendimos cuando nos dimos cuenta que el 80% de las solicitudes para validación de DNSSEC es que están siendo validadas por los resolutores porque había algunos de los ISPs que utilizaban resolutores públicos.

Y eso es completamente diferente de la firma a través de la zona. Por eso pregunto, ¿dónde está el programa de roadshow del DNSSEC?

DAN YORK: Usted tiene razón. En algunas estadísticas no sé Wes si está en APNIC, pero hay algunos países que tienen unos niveles extremadamente altos de validación de DNSSEC y cuando uno explora esto se debe a que algunos de eso ISPs en los países utilizan DNSSEC públicos, no tienen sus propios resolutores. Están usando 8.8.8, 1.1, 9.9 son algunos de los resolutores públicos que están presentes.

En cuanto al roadshow de ICANN no lo sé vamos a tener que responderlo después porque no estamos involucrados en ese programa directamente, por eso vamos a tener que responderle después. Yazid denos por favor su nombre a alguno de nosotros y lo vamos a responder después. En cuanto a la documentación

encuéntreme después y le voy a hablar, la Sociedad de Internet publica información en distintas partes de sitios web, también ICANN ha publicado.

Hay varios recursos disponibles para hablar de los detalles en muchos de los servidores autoritativos. Vemos que ellos han creado su propia documentación para poder hacerlo, es decir, que hay unos buenos vínculos para poder responder. ¿Alguna otra pregunta? El caballero que está por ahí.

ORADOR NO IDENTIFICADO: Gracias. Quizás esté un poco fuera de tema, pero quiero saber ¿cómo el DNSSEC se comunica con la respuesta Sig cero?

WES HARDAKER: No hay ningún tipo de conexión. DNSSEC que está diseñado para proteger un conjunto de datos y hacerlo verificable para que sin importar como llega uno lo pueda entender. Sig cero y TSIG es otra tecnología dentro del DNSSEC, pero solamente aseguran una conexión, no los datos en sí sin importar qué ruta tomen son distintas tecnologías.

DAN YORK: Muy bien.

WARREN KUMARI: Es algo que tiene que ver, el DNSSEC permite validar la información independientemente en la manera que llegue. Una de las cosas

interesantes que surge de eso es que una serie de personas están descargando toda la zona raíz en el resolutor porque está todo firmado y no hace falta mandar a consulta a la raíz es una de las cosas lindas de tener una zona firmada en ciertas circunstancias, simplemente se tiene todo el archivo de la zona o si no lo hace otra persona.

ORADOR NO IDENTIFICADO: Con la solicitud de transferencia.

WARREN KUMARI: Muchas de las notas B, N y F, no sé qué otra puede hacer AFXR, eso se llama rutas locales, esto es uno de los nombres, el RFC 7706 ahí hay información y va a haber una versión nueva de esto pronto.

WES HARDAKER: Ruta local o híper ruta local, ahí se puede hacer a través de localroot.isi.edu, nos permite tener un resolutor donde está todo en pre cached y facilita las cosas si es un administrador que sabe hacerlo, no para el usuario final

ORADOR NO IDENTIFICADO: No se identifica, si .com tiene 12 servidores de nombres y cada uno tiene una clave individual de DNSSEC para cada máquina para todo el TLD.

WARREN KUMARI: Se puede poner en cualquier servidor de nombres, esto es especialmente lindo si uno tiene un servidor de nombre propio y se tiene a otra organización que tiene uno secundario, claro uno firma la zona y permite que los demás tengan otras claves según sea necesario y no hace falta preocuparse por eso.

DAN YORK: Eso es lo bueno porque una vez lo tenemos todo firmado ya podemos ponerlo en cualquier lugar en una clave privada o pública, criptografía. ¿Alguna otra pregunta? Pueden ser generales, pueden ser tontas, pueden ser de DNSSEC, de SEC, de lo que quieran. Sí, adelante.

YAZID AKANHO: Otra pregunta. Escucho que hay investigación o análisis en desarrollo para cambiar el protocolo para generar las claves públicas o privadas de la zona raíz, ¿dónde están esos debates? ¿Y qué es lo que sigue?

DAN YORK: Creo que algunos de mis colegas de la mesa pueden responder, pero en breve en la firma cuando tenemos la firma y el servidor de firma se firma utilizando un algoritmo criptográfico específico de RSA o criptografía de curva elíptica o alguna otra cosa. Y estos algoritmos tienen propiedades distintas en cuanto a ser más seguros, algunos de los protocolos originales han sido alterados de alguna manera, ha habido intrusiones.

Entonces las claves de RSA 2048 y la curva elíptica que son más pequeñas hay distintos algoritmos existentes. En cuanto al estado de la raíz… Me imagino que tú quieres hablar, ¿sí? Está pulsando el botón querido mío, sí.

WARREN KUMARI: Hay mucha religión respecto del protocolo criptográfico básico, si ponemos tres especialistas van a apuñalar a los demás diciendo: "Que el tuyo es mejor" "que el RSA o el elíptico o ED 25519…" En este momento ha habido alguna migración de RSA, algunos protocolos más nuevos, pero una de las cosas que están empezando a comentarse son los protocolos de seguridad quantum. Tienen alguna preocupación de que las computadoras cuánticas van a hacer que la criptografía existente no funcione.

Hay una serie de personas que dicen que es exagerada esta preocupación, pero la gente está empezando a considerarlo en algún punto y quizás empiece a considerarse ese tema.

DAN YORK: No hay del lado de raíz un pedido inminente de cambio de protocolo. Russ.

RUSS MUNDY: Voy a hacer promoción de nuestro taller del miércoles, el programa tiene una presentación de Kim Davies sobre los planes del siguiente rollover de KSK de raíz. Si le interesa más información sobre detalles de

cuándo, cómo y los distintos aportes de la comunidad el taller del miércoles en la tarde de DNSSEC, creo que una sesión de 20 a 25 minutos donde Kim que es el presidente del PTI que está a cargo va a hacer una presentación del plan del borrador reciente, creo que salió el viernes o el sábado.

DAN YORK: Ese taller va a ser a la 1:30 de la tarde, hay horas de debates de distintos tipos en la sala de al lado sobre DNSSEC de todo tipo, algunos son de alto nivel o intermedio o básico, así que verán a algunos de nosotros que van a estar trabajando en ese tema. ¿Alguna otra pregunta?

Está Andrew con el micrófono en la mano, ¿alguna otra pregunta? Hay asesoramiento gratuito a esta hora, de lo contrario vamos a decirle a Warren que empiece a hacer bromas. Perfecto, ¡bien! La amenaza sirvió.

ORADOR NO IDENTIFICADO: Quizás la pregunta sea tonta, pero quisiera aclarar algo en mi cabeza, es como una especie de seguimiento de una pregunta previa. Básicamente si no tengo un buscador que soporte DNSSEC como Outlook o lo que fuera, ¿quiere decir eso que la sección entre mi resolutor de DNS y mi cliente está técnicamente sin protección?

DAN YORK: Sí. Todas las aplicaciones en su equipo históricamente, siempre ha dejado la resolución de DNS a un programita, el stub resolver del

sistema operativo que hacía consultas con el resolutor del ISP y las cosas que hacían falta. El sistema operativo no soportaba la validación de DNS, la verificación de la firma o sea estás en riesgo de que el Dr. Malito te mandé información falsa que te redirija a otro lugar. Históricamente había sido así.

A parte de algunas otras cosas como ejemplos que hay que la gente agregó en la validación de DNS buscadores específicos más que nada para prueba, esto está cambiando hay todo un grupo dentro del ITF que está considerando el hecho de que hay más y más aplicaciones que hacen DNSSEC.

Entonces lo que hablamos del DoH y los buscadores de la red son parte de estos problemas y aplicaciones que están trabajando más con validación de DNS de manera que están cambiando la arquitectura sobre cómo funciona DNS y también la internet. Warren me está mirando como que quiere decir algo, sí Warren.

WARREN KUMARI: Piensan que quizás estamos sobrevendiendo la protección. Si vemos en el skit el ISP va por la validación y eventualmente vuelve y dice: “Validé esto, no te preocupes está bien”. La manera en que funciona DNSSEC es que la validación del ISP o lo que sea hace la validación y le dice al cliente que lo hizo y que hay que confiar en él, básicamente dice: “Sí, está bien estoy contento”

Eso significa que si el paquete se manipula volviendo del resolutor al cliente alguien podría estar haciendo cosas malas, al fin y al cabo, sería

bueno que la computadora validara a perse si no confiara en el ISP directamente y si no que hiciera todo el trabajo criptográfico a perse. En algunos sistemas operativos se les puede forzar a hacerlo, Linux, por ejemplo, muchos de los Debian uno tiene la posibilidad de activarla o no a la validación propia.

Y hay software que se pueden agregar a la máquina que se llama stubby que hace la validación en la computadora. Y en general, uno confía en el ISP para que el resolutor verifique y tampoco que manipule los datos de vuelta, ¿no?

ORADOR NO IDENTIFICADO: Estaban pensando un poco más en tener a alguien en la red local que está envenenando todo, está filtrando y responde más rápido a la consulta de DNS.

DAN YORK: Eso es lo que puede pasar y pasa mucho también con la privacidad de DNS sobre TLS, DoH, estas cosas, para ver cómo encriptar la conexión desde su esquipo al resolutor recursivo para poder tener una conexión segura y por supuesto, puede estar una persona local. Es otro elemento de defensa, una capa adicional de protección de DNS.

WARREN KUMARI: Hay dos ataques distintos. Tienes a alguien en tu red que está envenenando y te da respuestas envenenadas para forzarte a ir a un lugar erróneo, pero también tenemos algo que da igual miedo es que

alguien está observando tus paquetes en la red y no ayuda si tienes https://alcólicosanónimos.org o Human Rights Watch.

El hecho de que estás resolviendo ciertos nombres potencialmente es algo tan dañoso como ver el contenido que estás mirando.

RUSS MUNDY: Esto se llamó "el ataque de la cafetería" donde uno se va a una cafetería local, la Wifi de ahí puede estar encriptada, pero es accesible, libremente cualquiera que está en la cafetería puede conectarse, hacer copias o dar respuestas engañosas a tus consultas de DNS. Entonces si tienes un medio de protegerte, proteger tu máquina donde confías la información, vas a ser menos vulnerable a ataques y sé de hecho que esto es algo realizable y que hay software ya disponible para descargar en internet que te permite hacerlo.

DAN YORK: DNSSEC tiene que ver con verificar cuando recibe la respuesta correcta, integridad, lo que venimos hablando acá, cada paso adicional de mejoras de privacidad y hablaremos eso el miércoles a la 1:30 p.m. vamos a hablar de este tema.

ORADOR NO IDENTIFICADO: Sí. Muchas gracias.

DAN YORK: Kathy me dice que hay alguien en línea.

KATHY SCNITT: De Cosi. Podemos hablar de Cloudflare, Firefox y el resolutor de DNS respecto de la presentación previa.

DAN YORK: No estoy muy seguro a qué profundidad queremos llegar.

WES HARDAKER: ¿Lo puedo responder de manera neutral? El problema es que iba dar la charla en la conversación previa, pero si me equivoco, digan. Vamos a ir un poquito para atrás y a responder la pregunta previa rápidamente, hay múltiples maneras de proteger la conversación entre ustedes y el Dr. Malito, y también de protegerte de la conexión entre voz y el resolutor. En dos semanas va a haber una charla importante sobre el tema, pueden hacer DNSSEC en el cliente pueden usar DoH, DoT…

Hay una serie de maneras de ver cómo protegerlo y todos funcionan de distintas maneras. Para los buscadores como ya saben HTTPS comprende el protocolo, cómo utilizarlo, tienen velocidad en el uso decidieron qué quieren hacer DNS sobre HTTPS, están motivados para hacerlo y lo aplican de distintas maneras.

Yo pienso en dos en este momento, los otros son Chrome y Firefox, en Firefox lo anunciaron primero, decidió que iba a trabajar en conjunto con Cloudflare que es un proxy que tiene una serie de funciones y que están trabajando con DNSSEC, que están trabajando junto con ellos para mandar todas las solicitudes o consultas a Cloudflare.

Si están utilizando Firefox, si están en Estados Unidos va a haber planes inciertos hoy por hoy, pero están probando en Estados Unidos este mes con Cloudflare en este momento, pero van a ir yendo uno por uno con otros proveedores, Google por otro lado y corríjanme si me equivoco, está haciendo pruebas de ISP que brinde HTTPS con DNS.

Si están en una lista de confianza van a utilizar dos para comunicarse con el ISP, si no resultan ser válidas van a ir a DNS regular no lo van a mandar al tráfico a un tercero y eso ha cambiado recientemente.

WARREN KUMARI: Básicamente todo es correcto, aunque me duela. El enfoque de Chrome Google considera que hay que hablar con el resolutor actual porque potencialmente hace cosas como protección contra el malware, hablando con los resolutores actuales sin cambiarlo nos permite todas las protecciones, la búsqueda de DNS internos y este es el enfoque de Google.

DAN YORK: Para el que preguntó remoto es importante también comprender que hay un protocolo DoH, DNS sobre HTTPS definido por el ITF, RFC 8484 son protocolos sobre de cómo hacer DNS sobre HTTPS. El protocolo se llama DoH, el cliente que puede ser un buscador y en la audiencia primaria en este momento se puede comunicar con cualquier servidor DoH y es una manera de tener una conexión segura encriptada entre esas aplicaciones y un resolutor de DNS, ya encriptando esa conexión entonces DoH como protocolo es eso.

DoH como se instaló inicialmente en sus estadios iniciales, de ahí viene alguna disputa por los distintos mecanismos y las distintas maneras en que lo encara la gente, es importante comprender que hay un protocolo que funciona en esta capa de privacidad para verificar que alguien de la cafetería no capture todos tus metadatos de todos los lugares a los que quieres ir. Y eso que DoH y DNS sobre TLS que están, esos dos protocolos fueron designados para proteger la privacidad.

Incrementan el nivel de privacidad que tenemos y ahí aparece alguna disputa sobre cómo se implementa de distintas maneras en estos primeros días. Warren, ¿quieres acotar algo?

WARREN KUMARI: Wes había dicho "divulgación completa para Google" quería decir lo que hace Chrome.

RUSS MUNDY: Se va a escuchar más sobre este tema. En ICANN 64 hubo una sesión de alto interés de una hora y media o dos sobre el DoH y se mencionó DoT, pero fue una sesión larga está grabada y estoy seguro de que está disponible en ICANN 64 en el archivo en internet, tienen un par de horas de charla muy relevante sobre este tema.

DAN YORK: ¿Alguna otra pregunta?

ANDREW MCCONACHIE: En ICANN 65…

WES HARDAKER: ¿En Marrakech?

ANDREW MCCONACHIE: Sí.

WES HARDAKER: Debo decir que trabajo para la universidad del Sur de California.

WARREN KUMARI: Hay más material sobre DoH y DoT, hay algo similar en el taller de DNSSEC.

WES HARDAKER: Creo que hay un taller de DoH el miércoles.

DAN YORK: ¿Hay alguna otra pregunta? Aquí, adelante el caballero.

ORADOR NO IDENTIFICADO: Soy una persona de Estados Unidos. ¿Hay alguna forma de hacer consultas de DNS privadas que no sean identificadas en un café? ¿Por qué la consulta del DNS en sí está encriptada?

DAN YORK: Sí, de nuevo aquí es donde DOH o DOT, todas esas tecnologías te permiten hacerlo, si quieren hacerlo directamente lo pueden hacer a través de Chrome o Firefox como navegadores, se pueden configurar ahora para utilizar DoH y después decir a qué servidor conectarse, es decir, que lo pueden hacer ahora mismo.

También pueden ir a DNSprivacy.org, DNS-privacy.org donde hay todo un conjunto de programas de software, se puede instalar algo que se llama stubby en los sistemas locales que van a encriptar todas las consultas a un DoT específico. Es decir que podemos hacerlo, también pueden operar su propio DoH o DoT y lo pueden configurar de esa manera.

WARREN KUMARI: Y también se puede utilizar una VPN si quiere una solución rápida.

DAN YORK: ¿Más preguntas allá atrás?

ROCIO DE LA FUENTE: Mi pregunta tiene que ver con la inteligencia digital. Seguramente cuando hablamos sobre educar al usuario o al registratario deberíamos explicarles la importante de DNSSEC para sus dominios cuando se registran porque cuando hablamos de los ISPs, de los registros, no registradores sino registros, cuando hablamos de eso, ¿ayudaría esto a la implementación de DNSSEC? ¿Qué opinan ustedes?

DAN YORK: Bueno, yo creo que los cuatro diríamos que absolutamente si, nosotros alentamos a la gente a que lo incluya como parte de su implementación, debe estar firmado. Parte de los registradores, no sé qué pase en Argentina, pero algunos de los registradores han llegado al punto en que DNSSEC es simplemente marcar un casillero y en un mundo ideal ahí es donde queremos llegar nosotros desde el punto de vista de la firma.

Es decir que se convierta en algo simple, que el usuario final ni siquiera tenga que involucrarse en esto de ninguna manera, pero nosotros alentamos a la gente a que lo firme porque esto desde el punto de vista de la marca, de la reputación asegura que la gente va a recibir el aporte que necesita el DNS.

WARREN KUMARI: ¿Puedo estar en desacuerdo? Por favor.

DAN YORK: Sí, por supuesto que sí, a Warren le encanta discutir.

WARREN KUMARI: Depende en qué parte del ciclo de esta inclusión digital estamos hablando, yo creo que DNSSEC es algo bueno, pero habría que ver si es lo más importante para un nuevo usuario de internet, probablemente no. ¿Es lo más importante cuando alguien registra un dominio? Bueno puede ser, pero hay muchas otras cuestiones de seguridad que también

son muy importantes, entonces esto de algún modo encaja en un espectro.

DAN YORK: Muy bien Warren, este fue un espectro de desacuerdo.

ROCIO DE LA FUENTE: Yo estaba pensando en eso porque cuando uno piensa en los incentivos, nosotros de alguna manera estamos involucrando a ICANN y a la gobernanza de internet, entonces si no hay una formación técnica hay que dedicarle tiempo y esfuerzo en entender por qué DNSSEC es importante. Entonces el registratario o el usuario que está pensando en su compañía o en lo que fuere, ¿cómo podemos construir una narrativa? Para decir: "Bueno esto es importante, quizás el dominio va a ser un poquito más caro, pero ayuda a la seguridad de internet".

DAN YORK: Esto es parte del desafío, por eso en muchos lugares estuvimos trabajando con los proveedores de DNS, los registradores y alentándolos a que esto pase, es decir firmar todo como algunos proveedores hacen, es decir, ellos lo firman por defecto o hacer que sea más fácil que la gente entienda y que lo haga e idealmente hacerlo sin ningún costo, los modelos varían en los distintos lugares.

Yo estoy de acuerdo con Warren, en el gran esquema de cosas cuando alguien se pone online, esta es una de esas cosas que tienen en la lista, dependiendo del nivel de conocimiento y de capacidad quizás no esté

en el tope de la lista, pero idealmente eso es algo que está en la infraestructura, es algo que está a esos niveles. ¿Va a estar en desacuerdo una vez más Warren? Muy bien, ¿otras preguntas? Tenemos tiempo para una o dos preguntas más, ¿no? El Sr. Levine acá, conozco muy bien a John.

JOHN LEVINE: Este es un comercial en realidad. Más temprano algunos de ustedes mencionaron lo que la criptografía cuántica puede hacer, cuál es el efecto que puede tener en DNSSEC y por sorprendente coincidencia, hay una charla sobre ese tema, es el día técnico de mañana. Lo malo es que la persona que lo da es un tonto, pero no hay mucho que se pueda decir de eso.

DAN YORK: Muy bien John.

WES HARDEKER: Suponemos que es usted John.

DAN YORK: Muy bien, John va a dar una charla mañana al final del día técnico. Veo varios fellows aquí, mañana es el día técnico donde hay muchas sesiones que ocurren en una de estas salas, no sé cuál, fíjense en el cronograma.

Hay muchos temas que van desde criptografía cuántica hasta ataques DDoS, son distintos temas, no miré el cronograma de esta semana así que ni siquiera lo sé, pero hay muy buenas sesiones que están dentro de ese día.

WARREN KUMARI: Es la sala 516C.

DAN YORK: Muy bien, perfecto lo encontramos. Comienza a las 10.30 de la mañana, ¿alguna otra cuestión? Muy bien, les voy a agradecer entonces por su atención y también si están interesados en trabajar pueden venir a conversar con nosotros, vamos a estar aquí unos minutos más.

Y de nuevo, el miércoles a la 1:30 p.m. en la 517C, vamos a tener un workshop de DNSSEC que va a cubrir distintos temas. Les agradezco entonces y que disfruten de su semana aquí en la ICANN.

[FIN DE LA TRANSCRIPCION]