BEIJING – DNSSEC para Todos – Guía para Principiantes
Lunes, Abril 08, 2013 – de 17:00 a 18:30
ICANN - Beijing, República Popular de China

JULIE HEDLUND: Bien, ya comenzamos con la grabación. Bienvenidos. Esta es la reunión 46 de la ICANN 46 en Beijing, China, y estamos en la sesión DNSSEC para Todos, Guía para Principiantes, y les pido por favor que se sienten adelante, porque vamos a divertirnos y van a ver y escuchar mucho mejor si se sientan acá cerca. Soy Julie Hedlund, soy personal de la ICANN, tenemos acá información de los presentadores y quisiera decir que voy a ir primero y voy a pasarle la palabra a Dan York de la Sociedad de Internet, que es nuestro maestro de ceremonia.

DAN YORK: Bienvenidos. Primero, ¿cuántas personas pueden escribir DNSSEC? A Bien, veo que estamos en el lugar correcto. Esta sesión es una sesión introductoria en la que vamos a hablar sobre qué significa DNSSEC, qué soluciona, cuáles son los problemas y cómo funciona. Para los que quieren más detalle, hay una sesión el miércoles, de 6 horas, con los detalles del taller de DNSSEC; tendremos información a nivel de detalle, pero hoy vamos a hablar sobre qué significa y cuáles son las promesas y la interacción. Así que aquí tenemos el detalle del programa de lo que vamos a hablar. Y está en todas partes, tenemos en todas las pantallas, tenemos muchos presentadores y voy a presentarlos. Tenemos a

Warren Kumari de Google, y él va a ser uno de los presentadores y actores; Russ Mundy de Esparta que las puede presentar; tenemos a Dan York y Julie Hedlund; tenemos a Norm Ritchie y Jacques Latour quien llegará al final y hay otras personas que van a jugar un papel importante más tarde y hay alguien que va a planear y planificar un rol malvado. Y hoy vamos a hablar de qué se trata DNSSEC y, por favor, escuchen, ya hablamos que el DNSSEC comenzó hace 10 años, pero tenemos una historia alternativa que les vamos a dar aquí. Así que vamos a remontarnos 7000 años atrás y decir que el DNSSEC cuando teníamos Aguina, ella vivía en una cueva en el Gran Cañón y ella quería ver qué es lo que había ahí. Y en la otra parte de la montaña tenemos a Og, y Og también vivía en una cueva en el Cañón y estaban ahí, pero no podían hablar mucho. Era muy difícil de ir de un extremo al otro del Gran Cañón, porque era muy extremo. Así que podían bajar y después subir la montaña hacia el otro lado y pensaron cómo poder comunicarse. Una vez, cuando estaban ahí vieron el humo que salía ya. Entonces, con el humo podían comunicarse. Desafortunadamente, alguien vino también y teníamos al señor Kaminski que era muy malvado y él quería participar en la conversación así que enviaba señales de humo también. Y Aguina estaba en un lado del Cañón y veía las conversaciones, las dos conversaciones en el mismo sistema y este Kaminski, vino y dijo “bien, tengo dos señales de humo y no sé cuál es la verdadera”, así que se empezó a preocupar. [Próxima diapositiva por favor]Así que bien, decidió bajar y quería saber cuál de las señales de humo era la correcta. Cuando estuvo ahí ella y Og fueron a consultar con los sabios de la villa y de la población y uno de ellos, Diffy, tuvo una excelente idea ¿qué es lo que hizo? Fue corriendo, fue al final de la

cueva y había ahí una arena azul que era solamente visible en la cueva de Og. Nadie la podía ver. Entonces ¿qué es lo que hizo? La puso en el fuego y lo que pasó fue que el humo se transformó en azul. Y ahora era, muy fácil, porque Aguina podía ver la otra parte del Cañón y podía saber que cuando había humo azul sabía que era la señal correcta que venía de Og. Cuando Kaminski trató de hacer esto, hizo el humo, pero no era azul, así que Aguina supo que con el humo azul tenía la conversación correcta y de esto se trata el DNSSEC, asegurarse que tengamos la información correcta y saber que es la correcta información que necesitamos. Estamos buscando el humo azul, así que Warren nos va a dar ideas de cómo funciona todo esto.

WARREN KUMARI: Bien, ¿todo el mundo entiende cómo funciona el DNSSEC? Debemos entender cómo funciona el DNSSEC. Así que ¿quién entiende bien cómo funciona el DNS y qué es? Bien, algunos, pero no todos. Primero ¿qué es el DNS y qué es lo que hace? Simplemente, el DNS convierte los nombres de dominio tales como www.bigbank.com en números (direcciones de IP) 1.2.3.4, por ejemplo. Y la computadora resuelve el nombre y comienza con la raíz el DNS y cada uno de los niveles y le dice "¿Cuál es el nombre de dominio de www.bigbank.com?" Y lo envía al próximo nivel**.** Y en este ejemplo buscamos "www.bigbank.com" y dice "Quisiera la dirección de IP de www.bigbank.com" y el servidor dice "yo no sé dónde están los servidores de punto.com, ellos sí saben, pregúnteles a ellos". Así que bien, "quiero saber dónde está el www.bigbank.com", y dicen "No, pero lo que es más seguro es bigbank.com". Sé la dirección, hay que preguntar al resolutor y le

pregunta al servidor “quisiera la dirección de IP de www.bigbank.com,” y el servidor de nombres dice: “Ahora lo sé. La respuesta es 1.2.3.4,” y de todas maneras, la computadora se puede conectar con el servidor de. Sí, acá tenemos un ataque de “spoofing”. Tenemos varias conversaciones en la línea. No sé si esto es una conversación más interesante que la nuestra. Básicamente, el resolutor sabe dónde está la raíz y a cada uno de los niveles del DNS lo guía al próximo nivel y esta e a delegación al próximo, hasta tener la respuesta. Y, obviamente, algunos nombres son más populares que otros. Por ejemplo, www.google.com o www.yahoo.com o www.baidu.com. Y es muy poco eficiente hacer cada una de las preguntas y el resolutor recuerda la respuesta por un tiempo, está en caché. Una vez que le hacen a misma pregunta, ya tiene la respuesta. Y esto es mucha información que sale rápida y hay muchas personas que tienen la respuesta. Y vamos a demostrar esto con una pequeña obra de teatro.

[Tenemos interferencia en la recepción de sonido en inglés]

JULIE HEDLUND: Hasta que solucionemos el problema de interferencia, nuestros actores se van a poner las ropas correspondientes, pero vamos a tratar d solucionar esto.

WARREN KUMARI: Julie, yo necesitaba una remera un poquitito más pequeña, porque es bastante grande esta.

JULIE HEDLUND: Estamos en pausa todavía con la interferencia. Por favor, desenchufen al orador. Muchas gracias, ahora vamos a continuar con la obra.

DAN YORK: Bien, vamos a divertirnos un poco. Es difícil describir el DNS y el DNSSEC, es un tema bastante técnico y aquí tenemos expertos distinguidos que se transforman en actores. Lo que vamos a hacer es actuar una transacción de DNS con diferentes actores. Este es el Acto Nº1. Yo soy el Usuario Joe, el usuario típico, acá tenemos al proveedor de servicios de internet ISP, tenemos la raíz, tenemos el punto.com y tenemos a bigbank.com. Este primer acto es el siguiente: Yo soy el Usuario Joe y quiero hacer mis transacciones bancarias. Así que quisiera pagar las cuentas, las facturas.

USUARIO JOE: Sr. ISP, quisiera ir a www.bigbank.com.

SR. ISP: Muchas gracias, pero no sé dónde está el www.bigbank.com, primero le pregunto a la raíz dónde está bigbank.com.

RAÍZ: Muchas gracias, dice la Raíz, ¿por qué no le preguntan a punto.com? a 1.1.1.1.

SR. ISP: Le preguntamos entonces a punto.com dónde está www.bigbank.com

.COM: Yo no sé, pero por favor pregúntenle a bigbank.com; esto es 2.2.2.2.

SR. ISP: Gracias. Bigbank quisiera saber dónde está www.bigbank.com.

BIGBANK: Sí, yo sé dónde está. Está en 2.2.2.3.

SR. ISP: Muchas gracias. Y ahora le doy la respuesta a Joe, el Usuario, entonces, la dirección es 2.2.2.3.

USUARIO JOE: Muchas gracias Sr. ISP. Ahora puedo hacer las transacciones de banco y mi computadora sabe que www.bigbank.com es 2.2.2.3. Ahora sí puedo pagar todas mis facturas y mis cuentas.

WARREN KUMARI: Nadie pidió un bis a Dan. ¿Qué es lo que pasa? ¿Qué significa esta presentación de Dan? Entonces, Aguina actúa como resolutor y Og es el

servidor, entonces, cuando el malvado Kaminski envía señales de humo, Aguina se confunde y el resolutor no sabe cuál de las respuestas es correcta. ¿Y qué es lo que hace DNSSEC? DNSSEC le pone el humo azul, le provee al resolutor la respuesta correcta. Entonces, ¿Por qué se necesita esto? Cuando el DNS fue diseñado originalmente, hubo un problema de escalabilidad. Internet era mucho más pequeña y segura. No se necesitaba tanta seguridad; la mayoría de la gente conocía a las demás personas, no había en todo el mundo, así que no había chance de que alguien tuviera una conducta maliciosa. Así que no había protección en cuanto a "spoofing" o suplantación de identidad. Como Kaminski, por ejemplo, que pretende ser Og. Y una vez que se saben las respuestas correctas, el resolutor recuerda la información durante un tiempo en memoria cache. Entonces el DNSSEC lo soluciona a través de firmas digitales. Cuando uno le pregunta a un servidor de nombres la respuesta, le da el próximo nombre en la cadena y firma la respuesta. Y ya que está firmada, uno la puede creer. Y ahora que el resolutor sabe cuál es el servidor de la raíz, sabe cuál es la clave de raíz. Y la raíz es la información que genera la firma y se crea una cadena de confianza. Entonces, ante la pregunta sobre cuál es la dirección de "Cual es la dirección de www.bigbank.com", la raíz da la respuesta con respuesta firmada y va al dot.com y a los diferentes niveles. Y el dot com dice "Yo no sé y lo que sé es dónde está el servidor de nombres de bigbank y lo firma", y el resolutor puede chequear cada uno de los niveles y en cada uno de los niveles existe una firma para pasar al siguiente. Básicamente aquí ¿queremos presentar esta diapositiva o queremos saltearla? Bien, esta es la siguiente entonces. Obviamente, es más complejo que la

descripción del DNS y así, de esta manera, vamos a demostrar cómo funciona el DNSSEC.

ACTO 2

DAN YORK: Ilustrándolo con el Acto 1 y lo que presentaba Warren, DNSO es insegura inherentemente. Y vamos a ver lo que es un ataque y el hombre en el medio del ataque. Es un incentivo para el desarrollo de DNSSEC. Vamos a repetir lo que hicimos antes, vamos a volver a la banca y vamos a demostrar cómo es el ataque.

USUARIO JOE: Más cuentas que pagar. Sr. ISP, quiero ir a www.bigbank.com.

SR. ISP: Gracias. No sé dónde queda, pero vamos a preguntarle a la raíz.

RAÍZ: Gracias por preguntar, pero tampoco tengo idea. Tienes que hablar con punto.com en 1.1.1.1

SR. ISP: Voy con.com, ¿Sabe dónde queda bigbank.com?

.COM: Perdón, no. Pero sí sé que el nombre del servidor para bigbank.com es 2.2.2.2. Así que tienes que preguntar allí.

SR. ISP: Lo haré. Hola bigbank. ¿Tienes la dirección de www.bigbank.com?

BIGBANK: Sí, claro que la tengo, la dirección de bigbank.com 6.6.6.6.

SR. ISP: Muchas gracias. Acá tienes Usuario Joe, la dirección de bigbank.com es 6.6.6.6.

USUARIO JOE: Gracias Sr. ISP, ahora puedo ir a hacer los trámites y pagar mis cuentas en bigbank.com y espero que nadie me esté tocando los bolsillos.

DAN YORK: Eso es Acto 2 y se llama El Hombre Bajo Ataque", y el de acá se llama el Dr. Malito que inyectó la respuesta antes de que bigbank lo pudiera hacer y es así como esto funciona. Ahora vamos a implementar DNSSEC, quizás habrán notado que hay dos servidores; uno es el de publicación de información, estos chicos, Sr. ISP. El otro es el que lee información. Tenemos que desarrollar alguna manera de autenticar la información

recibida. Vamos a desarrollar una cadena de confianza, de eso se trata. Firmo, aquí está mi firma.

SR. ISP: Hola Raíz, me gustaría hacer esto de DNSSEC, acá está la información, para que creas que soy yo.

RAÍZ: Maravilloso, confirmo que tú eres tú mediante la estrellita.

SR. ISP: Hola aquí.Com. Firmé mi zona, estoy en bigbank.com y he sido habilitado por DNSSEC y tengo la tarjeta establecida.

.COM: ¡Qué bien!

DAN YORK: Lo que pasó ahí es que tenemos una cadena de confianza. Se autentican entre sí y se pasa la firma digital entre ellos. Con la jerarquía firmada, repetimos El Hombre Bajo Ataque y veamos qué pasa.

USUARIO JOE: Más banca, más cuentas. Sr. ISP, quiero ir a www.bigbank.com.

SR. ISP: Perfecto, no sé dónde queda bigbank.com, pero vamos a preguntar a raíz. Y saben que tengo esta estrellita que valida para saber que es la raíz.

RAÍZ: No sé dónde queda bigbank, pero puedes ir al servidor punto.com que está en 1.1.1.1 y que acá está su firma.

SR. ISP: Bien, está bien. La firma es correcta, gracias. Quiero ir a www.bigbank.com, ¿sabes dónde queda?

.COM: No, no sé, pero sí sé dónde está bigbank.com y puedo firmártelo.

SR. ISP: Gracias. La información está bien Bigbank, quiero la dirección de www.bigbank.com..com.com.com

BIGBANK: Hola, la dirección para www.bigbank.com es 6.6.6.6.

SR. ISP: ¡Eso está mal, no está validado, tómatelas!

BIGBANK: Bueno, menos mal que preguntaste. Yo soy bigbank.com y la dirección de www.bigbank.com que es 2.2.2.3 y ya está firmado.

SR. ISP: Sí, está bien, muchas gracias. Acá, Usuario Joe, tienes la dirección 2.2.2.3 y está validado.

USUARIO JOE: Gracias Sr. ISP, ahora puedo hacer mis trámites bancarios sin preocuparme que nadie me estafe. Gracias.

WARREN KUMARI: Como verán, hemos practicado ampliamente nuestra actuación. Así que le paso la palabra a Russ por una muestra de implementación de DNSSEC y la guía de las opciones de instalación.

RUSS MUNDY: Siempre me entusiasma hacer esto, como sabrán, nos divertimos. Esperamos que ayude a explicar las distintas actividades diversas que implica DNSSEC. Y aunque cuando mira los detalles específicos, hay muchos detalles complejos que hay que considerar, cuando uno piensa ¿qué es lo que hace ICANN para comenzar a implementar DNSSEC? Y la

respuesta en casi todos los casos es depende de lo que uno hace con las DNS. Si uno es un operador y hace DNS como punto focal del negocio, como por ejemplo el operador de un registro o un ISP y proveedor de nombres de servicio y registro. Se hacen muchas cosas al nivel DNS y hay diversas cosas que se pueden utilizar para comenzar. Si uno tiene una actividad tipo empresa, hay una serie de cosas que son un poco distintas. Lo que tiene que hacer es examinar lo que tiene que hacer ahora y cuáles son las partes involucradas. Que es lo que vamos a tratar de cubrir hoy.

Si, por ejemplo, son un registro, con una gran operación de TLD probablemente tengan personal profesional de DNS, en cuyo caso, seguramente estarían hoy hacienda todas las actividades con el personal actual interno. Quizás estén profundamente calificados, si tienen otra empresa que hace cosas importantes con DNS, pero terceriza muchas cosas y tienen algunos proveedores externos que hacen DNS. Uno querría que establezcan que pueden hacer DNSSEC, porque muchos de ellos están empezando a trabajar con el proceso y algunos no han comenzado para nada. Si tienen una actividad que hace cosas a nivel lateral y DNS no es el punto focal del negocio, sigue siendo importante, pero no es lo principal. Quizás estén operándolo ustedes como algo colateral, porque no implique demasiada energía o quizás lo tercericen totalmente. Independientemente de lo que hagan, fíjense en lo que hacen con DNS hoy. Si son como Jacques, uno de mis ejemplos favoritos es un paso que se utiliza mucho en DNSSEC, hay en Estados Unidos una empresa denominada Comcast, que es un ISP y todos los servidores que prestan servicio a los usuarios están dentro de DNSSEC hoy. Y las cosas

que hicieron para implementarlo para sus clientes son un poco distintas de lo que hace de pronto VeriSign que es el operador de.com and.net, o Affiliates con eso de punto.org. Hay que considerar lo que se hace y cómo. Y esta es la primera etapa, la etapa de planificación e investigación sobre lo que se está haciendo y cómo. Si son una empresa – diapositiva siguiente – si son una empresa – Ay, no veo bien, a ver si puedo entender qué dice] HP [ya entendí], empresa grande, mucha experiencia en DNS. Creo que lo hacen a nivel interno, pero hacen mucho DNS. Están bajo.com, así que está todo listo, pueden firmar su zona y todas las zonas que tienen administradas bajo su paraguas. Independientemente de la manera que hagan DNS hoy, estoy tratando de ilustrarles acá cuáles son las piezas específicas. Si son una empresa, van a estar operando con servicios de nombres recursivos o uno con autoridad o, como decía Norm los proveedores de información para las zonas propias, entonces, pueden estar considerando la firma de las zonas propias, en cuyo caso, es la manera más efectiva de comenzar si uno es operador con servicio de nombres con autoridad, firmar las zonas. No se preocupen si hay otro que haga validación, pero manejen la firma y acostúmbrense a la parte DNSSEC de DNS, porque hay algunos cambios que implementar y uno de los más importantes es respecto de los DNS comunes. Los cambios que se tienen que dar, esta es la diapositiva de la montaña, como la llamo. La parte izquierda es lo que a menudo se llama la parte de provisión. Y ya sea que uno es una empresa o un registro o un ccTLD, todas estas cosas se aplican para cualquier zona única dada. Y a la izquierda tenemos donde está la información. Si uno es una empresa todo se puede dar dentro de la organización. Cuando uno maneja la conexión con el registrador, como por ejemplo

HP interactúa con el registrador que utiliza para llegar a.com, tienen que intercambiar información con el registrador, entonces, la información llegue a la punta del triángulo. Y después es usada, distribuida y consumida en la parte derecha. Hay muchos actores involucrados.

Como podrán ver en la diapositiva. Entonces, lo que hacemos es examinar las partes de los DNS, saber de dónde proviene el nombre, cómo se hace, quién presta ese servicio. Si es interno, el personal de informática, un personal especial o especializado en DNS o si lo da el registrador. O sea, puede venir de distintos lugares. La planificación de DNSSEC es importante ver de dónde provienen todas las partes de DNS que es el primer paso importante que queremos dar. Lo que vemos acá es otra manera de ilustrar como ingresa la información en los servidores de autoridad de los nombres. Y tal como se ilustra con Joe el usuario en la parte izquierda de la diapositiva en búsqueda de una respuesta.

Se lo puede considerar de manera sencilla o más compleja. Cuando miramos las dos hileras superiores ilustran la zona raíz, los servidores de nombres, hay 13 letras, pero más de 100 máquinas. Lo mismo para para.com, hay 13 letras. Y la página siguiente nos da un ejemplo de la cantidad de resoluciones que buscan los nombres, buscando una respuesta. La cantidad de veces que puede suceder. Esta gráfica se hizo con una herramienta de una de las cajas de herramientas para el mundo de la fuente abierta. En este momento había menos de 100 búsquedas y respuestas. Recientemente volví a verificar y hay bastante más. Hay como 120 en www.CNN.com, no tenía una imagen linda, pero esto es lo que pasa con CNN.com cuando hacemos una búsqueda.

Los datos de la zona son lo importante y eso es lo que queríamos mostrar antes. La dirección IP para www.bigbank.com, que no es 6.6.6.6, sino 2.2.2.3, y eso es lo importante. Eso es lo que hace DNSSEC; nos da la base técnica que puede aprovechar el usuario de la información de internet para tomar la decisión correspondiente. Volvemos al triángulo, vean lo verde. Ahí está DNSSEC, ahí está funcionando. Si miramos a la izquierda, si ingresamos información, está la parte de aprovisionamiento, si uno es usuario de un nombre y va a un registrador. El aprovisionamiento está de ese lado. Una vez que está en el servidor de nombres y ha sido firmado, es la información que la gente obtiene cuando hace preguntas y obtiene respuestas. Hay que tener mucho cuidado con el lado del aprovisionamiento, pero DNSSEC resuelve los desafíos de integridad de datos y de seguridad para verificar que la información provenga de un lugar seguro para la información de DNS. Si estamos haciendo DNSSEC de la misma manera que hacemos DNS, probablemente esa sea la manera adecuada de hacerlo. Tomamos lo que hacemos de DNS, no tratemos de tirar la operativa por la puerta y reemplazarlo por algo nuevo, porque agregamos más complejidad, porque tenemos que verificar que DNS es correcto antes que funcione DNSSEC. Si se fijan, esta es otra ilustración con un poquitito más de complejidad, pero bastante sencilla sobre cómo se hace. Acá tenemos lugares adicionales donde tenemos que agregar alguna pieza adicional. Es la parte de las estrellitas en la actuación que hicimos. Esa es la fecha de autenticación para que el consumidor de datos sepa que proviene del lugar correcto. Cuando tratamos de ampliar la operación de DNS actual, esto es lo que uno tiene que buscar. Las piezas que traen información a DNS y que sacan

de DNS, los detalles de las palabras, hay más texto en la pantalla que lo que voy a decir, pero si alguien quiere hablar del detalle, lo podemos hacer al final de esta reunión. Pasemos a la diapositiva siguiente. Y si la operación, tenemos software y hardware que provienen de un grupo de distintas cosas, tienen que ir a los proveedores del servicio que hacen las cosas relacionadas con los DNS para poder hacer DNSSEC, y si pueden ayudarlos a hacerlo. Y si no lo pueden hacer, con el DNSSEC ahí ustedes tienen que comenzar a obtener el DNSSEC por parte de alguien que pueda dar este servicio. Entonces, para su empresa, ya sea un operador de DNS o profesional, hay que asegurarse de que los proveedores de los productos y servicios van a soportar DNSSEC. Y así concluimos nuestra presentación formal. Ahora sí queremos que todos ustedes presentes hagan las preguntas y formulen las preguntas. Si ustedes piensan que somos totalmente estúpidos con nuestro actito, nos pueden decir, pero estamos ansiosos de responder las preguntas de ustedes y para eso estamos aquí, para responder las preguntas que ustedes puedan tener. El micrófono está abierto para todos ustedes.

AHMED: Soy Ahmed de Pakistán. Mi pregunta se refiere a lo siguiente: ¿Cuánto ralentiza el tráfico de la internet? ¿Tiene un efecto o no? ¿El tráfico de internet se ralentiza o no?

RUSS MUNDY: La respuesta es no. Tenemos la respuesta con firma cuando se hacen las queries, las respuestas son más largas, pero es muy poco el tiempo de

procesamiento, pero cuando se hace un benchmarking es menos del 0% y esto es para la parte del DNS y la otra parte no está afectada así que es negligible, es algo que no consideramos.

DAN YORK: Tenemos estudios en el impacto de los proveedores de los servidores de nombres autorizados. Un análisis efectivo fue hecho por Wright y se anuncia, hay muchas fórmulas, hay muchos temas específicos, pero para la zona individual pueden tener ese informe, no sé exactamente dónde está pero es accesible. Pongan su nombre y saben qué es lo que va a ser en cuanto al entorno. No tenemos tantos detalles de datos disponibles sobre la validación, resolutores de validación. Warren, ¿sabes cuántos hay por parte del Google DNS?

DAN YORK: No tenemos datos públicos publicados, pero son datos que se pierden.

RUSS MUNDY: Hay otros grupos que tratan de medir la validación y no tenemos un impacto significativo hasta este momento.

LENDAL MCDONALD: Soy Lendal McDonald, del programa de becarios. ¿Cuánto cuesta implementar el DNSSEC?

DAN YORK: Creo que la respuesta es “depende”. Depende de dónde se encuentra uno, cuán grande es la zona. Y Jacques analizó los procesos con punto.ca, pero depende del nivel de seguridad, del nivel de cuidado que tenemos que querer en cada entorno y el rango. Hay personas que hacen diseño de diferentes piezas con código de fuente abierta, con costo mínimo, hay otros a gran escala, con hardware con encriptado, otras salas separadas y esto implica un costo muy alto así que puede cambiar. Le doy la palabra a Jacques.

JACQUES LATOUR: Depende de los requisitos de seguridad, si usted es un ccTLD, un operador, una empresa, eso define básicamente cuánto va a gastar, de cero, de código abierto a muy caros.

WARREN KUMARI: Creo que hay un número de ccTLDs que lo hacen por cero. Hay que saber cómo hacerlo y saber que se está operando de manera estable. Pero los ccTLDs que tienen entorno complejo una personas lo puede hacer en algunos días si no tiene un costo mayor. Cualquier organización que lo quiera hacer lo puede hacer y es bastante fácil hacerlo sin costo.

DAN YORK: En muchas organizaciones los servidores de nombres autorizados ya están ahí. Y el DNSSEC tiene que ver con chequear un cuadro en la configuración. No se necesitan mayores cosas. Microsoft, Windows o cualquier servidor es bastante sencillo. Es agregar una línea a la configuración en esa parte, en la parte de validación.

RUSS MUNDY: Una de las cosas que quisiera decir en particular en esta pregunta es que, como ya dije en la presentación, es el contenido de la zona el que es importante. Esto es lo que se trata de proteger. Y, por lo tanto, usted debiera expandir el esfuerzo que sea razonablemente equivalente a cómo uno protege los datos de la zona en sí. Si tenemos un proceso bastante flojo para las personas que ponen y sacan nombres en y fuera de su zona con diferentes cambios, que no prestan atención a la precisión, no van a gastar muchos en DNSSEC, porque están gastando mucho más dinero en las partes encriptadas y ustedes no están protegiendo los contenidos. ¿Otra pregunta?

LEON: Soy León del programa de becarios, y tengo dos preguntas. La primera se refiere a si utilizar el servicio de Google público, ¿esto es un certificado seguro? y la otra pregunta es ¿cómo puedo yo como persona contribuir a reforzar el DNSSEC?

DAN YORK: Yo voy a tomar la primera. Google comenzó a hacer DNSSEC sobre sobre los resolutores punto.Google, pero es un lanzamiento básico. Le dan respuestas específicas a las preguntas específicas de DNSSEC. A veces, en algún momento en el futuro, cercano o no tan cercano esto va a estar disponible para todo el mundo. Si uno le pregunta a www.bigban.com va a tener una respuesta con DNSSEC. Y esto es similar a lo que ya se está haciendo en otras instancias como Comcast. Hay unas zonas más grandes y esto pasó hace poco y tienen algún problema con las claves de DNSSEC. La zona no valida porque están utilizando un servidor de DNSSEC. Tienen un ancla negativa y dice que damos una respuesta a pesar de que no validamos. Google está haciendo lo mismo y es claro que razón por la cual la zona no responde es que hay algún problema temporal que la persona no sabe y pueden dar una respuesta a pesar de que no es un DNSSEC seguro.

WARREN KUMARI: Las personas pueden hacer lo siguiente, si es propietario de un nombre de dominio, lo pueden firmar y una vez que lo firman, ustedes lo pueden hacer. Hay factores diferentes. De los 300 ccTLDs, unos cientos tienen firma, entonces sí son los cientos, el nombre de dominio puede ser firmado y puede hacer que funcione. El próximo paso es saber si el registrador soporta el DNSSEC. Y, en algunos casos, lo automatizan con un típico check, una cajita en la que hay que decir DNSSEC habilitado. Hay registradores que lo hacen automáticamente, no sé si lo hacen en el.br, pero sí sé que en algunas regiones, como en los Países Bajos, la

República Checa lo hacen y si usan.com,.net,.org tienen que saber si el registrador hace lo propio. La ICANN tiene una página en la que se informa sobre este DNSSEC. Como persona, uno puede ir a estos registradores y en algunos casos hay que preguntarle al registrador. Y en algunos casos muevo el domino, porque no quiero que esté firmado. Así que físicamente tengo que mover el dominio a otro registrador para que se haga. En cuanto a la validación, esto depende de cuán involucrado uno quiera estar, qué tipo de protección quiere tener. Tengo diferentes herramientas como DNNSEC trigger, que me da un resolutor validado en mi propio sistema. Entonces, yo lo puedo utilizar y la historia que contamos de la validación por el ISP, mi computadora lo hace. Es uno que yo puedo configurar para utilizar Google en este momento y cuando yo corro un software en el sistema, hace una consulta con Google. Hay dos cosas que se puede hacer, ya sea firmar los dominios en cuanto a las partes de la firma y en cuanto a la validación hay que ver si el ISP puede soportar el DNSSEC y si no lo puede hacer, le preguntan y si no, pueden instalar estos software. También hay algunos add-ons de Chrome y Safari e IE que les pueden brindar ciertas firmas de validación en ese entorno.

JULIE HEDLUND: Tenemos una lista e preguntas, hay una persona acá y acá y veo otra mano por allá. Así que tenemos cuatro en la lista de preguntas.

DAN YORK: Un agregado, si ustedes están operando sus propios nombres, los servidores de nombres para sus propios nombres y no tienen una cadena, ustedes sí lo pueden firmar, nada les impide hacerlo. Hay otras personas que no van a poder validar a menos que ustedes les den el "trust anchor", pero los nombres, ustedes los pueden operar en sí, pueden aprender e incorporarlos en los procesos de ustedes en este momento, el DNSSEC para las zonas firmadas autorizadas y no necesitan ir en una cadena hacia la raíz. Hay una cierta cantidad de capacidades, el DNSSEC las impulsa. El miércoles van a ver el tema de espacio de nombres DNS y el DNSSEC. Existen herramientas para hacer la validación del DNSSEC y si quieren estar involucrados, usen el feedback de los desarrolladores.

RUSS MUNDY: El documento está en la zona de URL, lo pueden chequear.

JIAN PUAN***00:48:48: Soy Jian Puan y trabajo en una empresa en China. Tengo dos preguntas. La primera ¿ustedes tienen datos que informen cuántos servidores o la tasa de los servidores que han empleado DNSSEC? Y la segunda pregunta se refiere a lo siguiente: ¿Si un servidor de DNS es controlado por un hacker, el DNSSEC puede ser utilizado en esa situación también? Muchas gracias.

RUSS MUNDY: En cuanto a la primera pregunta, hay diferentes puntos importantes. Lo más fácil es ver el despliegue en el mundo del ccTLD, hay un mapa con el despliegue del DNSSEC, con deploy360 que muestra la cantidad de ccTLDs que fueron firmados. Hay algunos problemas, pero probablemente esta sea la manera más visible de ilustrar el crecimiento, al ver los ccTLDs que fueron firmados, porque el mapa lo refleja para tener una idea del crecimiento. En cuanto a que un hacker controle un servidor de nombres, con el DNSSEC lo que se autentica en realidad, al usuario final, el usuario de esa información DNS, son los datos en sí, no de donde viene en esa máquina que envía los bits, de donde viene es el originador que lo puso en el DNS, y los servidores de nombres en el medio pueden tener cierta información que puede ser un spoofing o pueden tener información errónea en caché, tienen que darlo a un resolutor de validación que lo va a detectar y va a decir "no, estos son datos erróneos". Si el hacker puede controlar la máquina que hacía la firma, ellos controlan la máquina que hace la firma y sí, ahí puedes haber un daño. Pero si va la provisión donde los datos van antes de aplicar el DNSSEC, ésta va a tener la firma del DNSSEC que en ese caso el resolutor de validación no va a poder diferenciar, porque va a estar firmado y la debilidad yace en la parte de provisión, o sea, la parte izquierda del triángulo. Y aquí vemos el mapa.

DAN YORK: Este es un mapa que fue publicado y muestra la adopción en cuanto a la operación, los planes, los experimentos y esto lo importamos en la web. Hay diferentes mapas de diferentes regiones, hay una animación que muestra el desarrollo en el tiempo. Si ustedes tienen la chance de

participar en el taller del miércoles de DNSSEC, va a haber diferentes charlas referidas a estos temas. Por ejemplo, las tendencias en las estadísticas a lo largo del tiempo. Vamos a tener análisis preciso sobre estos temas.

JULIE HEDLUND: Quisiera saber, este gráfico, para los que no estuvieron en la sala, recomendamos que vayan y consulten la presentación del taller de DNSSEC del miércoles, porque ese gráfico no fue mostrado en la sala de Adobe Connect, es un mapa con colores que nos muestra todos los niveles de despliegue de DNSSEC y vamos a tener más el miércoles en el taller.

RUSS MUNDY: Muchas gracias, Julie. ¿Próxima pregunta?

MOHAMED: Hola, soy Mohamed, soy de Bahréin. Quisiera agradecerles por esta presentación tan general y tan abarcativa. Tengo dos preguntas en cuanto al DNSSEC. ¿Cuáles son las partes involucradas en las transacciones DNSSEC, hacia el usuario final? ¿O es un registro que implementa el DNSSEC? Y si el usuario final envía algo que sea nuevo o necesita una configuración especial, por ejemplo, una computadora portátil. Esta es la primera pregunta. La segunda se refiere a ¿por qué hay una firma entre la raíz y otras sub-raíces? porque esto ya está bien definido como usted demostró anteriormente, estas raíces están bien

definidas, la raíz del ISP va hasta el punto.com, ¿por qué debería firmar esta transacción si el servidor de dot.com está bien definido?

RUSS MUNDY: Quisiera responder la segunda pregunta primero. El DNS por naturaleza, recuerden las presentaciones, es una parte y baja, aquí lo vemos bien. Aquí vemos la estructura de información del contenido del DNS. Entonces, todo solicitante de información de salida de DNS o resolutor de alguna manera sabe dónde comenzar y cualquier resolutor que busca, hay una repetición recursiva, sabe dónde están los nombres de raíz, pero no tiene que saber nada más y sabemos que hay una cajita para la raíz, pero hay muchas máquinas que pueden darle esa respuesta, ya que DNSSEC, por la firma, es una parte integral del DNS, esa es la razón por la cual se firma la decisión que la información esencialmente es el equivalente alternativo a saber dónde están los servidores de nombres de la raíz y cuál es la clave publicada de la zona de raíz. Y así pasamos hacia abajo del árbol y de esa manera básicamente, esto va en paralelo con el servicio de nombres.

DAN YORK: Hay una respuesta más sencilla que está el Dr. Malito que puede presentar firmas, porque puedes ir y firmar la zona y presentarlo de manera tal que parezca que es. Pero lo llamamos la cadena de confianza global que verifica que cuando el ISP da la validación, verifica la firma hasta la raíz, como decía Russ. Por eso hace falta esta cadena, para que el atacante no nos dé algo que diga “bueno, es esto”, sino que...

WARREN KUMARI: A ver si puedo responderlo de otra manera, hay tres maneras de responder. ¿Cómo funcionan las firmas digitales? Criptografía pública. Tenemos clave pública y privada. Todo lo firmado con la clave privada puede ser desencriptado solo con esta clave, que vendría a ser como la firma. Cuando va la raíz, la raíz dice "conozco la respuesta que es www.bigbank.com", pero tenemos la clave que es pública y la firma que dice que es correcto.

MOHAMED: ¿Por qué el servidor de raíz no nos da la dirección de IP sin la clave? Porque son cosas bien definidas.

WARREN KUMARI: ¿Qué? ¿El servidor punto com está bien definido?

MOHAMED: El punto com, el punto org o el que sea.

WARREN KUMARI: Hay muchos TLDs distintos, entonces los punto.com son bien conocidos, cuando lanzamos uno nuevo, eso no es conocido de inmediato.

MOHAMED: Pero hay algunos que ya están bien definidos.

[Es una conversación entre podio y sala]

WARREN KUMARI: Básicamente, hay millones y millones de resolutores y solo una zona raíz con 13 direcciones, pero de esa manera los millones y millones y millones de resolutores, básicamente tienen que saber o conocer un conjunto de direcciones, no necesitan conocer 100 o 1000 o un millón. Hay más de un millón de zonas, mucho más. Como los resolutores ya tienen que saber dónde está la raíz, teniendo la raíz firmada, no hay nada que evite tener otras claves que uno conozca y que no tenga que validar en la raíz. Si confía en esas claves por una empresa o para un país si quieren tener todos los resolutores del país o de la empresa, que tengan la clave de la información pública en los resolutores no hace falta salir del ambiente, porque podemos trabajar desde ahí, pero es más complejo a medida que se incrementa el tamaño, entonces, mantenerlo pequeño con la zona raíz se considera el mejor abordaje para la internet global. Del mismo modo, no prohíbe una estructura a veces se las denomina “anclas confiadas” para un área pequeña.

DAN YORK: ¿Podría repetir la primera pregunta? Estamos un poco perdidos en eso.

MOHAMED: ¿Qué partes están involucradas en las transacciones de hasta el usuario final? Preguntaba.

RUSS MUNDY: La política es siempre importante y esto es ICANN así que es importante hablarlo. Hay actividades DNSSEC que nos hacen preguntarnos si hace falta una política ubicua y la conclusión en el diseño técnico y la comunidad de ITF fue que no, nosotros les vamos a decir cómo hacer la protección criptográfica, pero los requerimientos para lo que tiene que ser la política que lo rodea está fuera del alcance de la definición técnica. Hay una gran cantidad, especialmente en los ccTLD, hay muchas declaraciones de política que dicen "nuestra firma, nuestra zona necesita tal cosa", y se opera de tal manera. Pero no es una necesidad absoluta de tener una firma en la zona de DNSSEC.

WARREN KUMARI: Como con todas las preguntas que involucran a ICANN las políticas, la respuesta es un poco más compleja. Russ estaba hablando de las partes de aprovisionamiento del lado de la resolución, la gente involucrada es el servicio que maneja las firmas y el resolutor del ISP. Normalmente, las máquinas no hacen demasiado con esta información, pero mucha gente piensa que la máquina del usuario final también va a estar involucrada, entonces, en la parte de validación de DNSSEC, lo que pasa en la estación de trabajo local.

DAN YORK: Algunas personas están incluyendo la resolución en la aplicación. Hay gente que hace validación de DNSSEC dentro de las aplicaciones otras dentro de la parte de administración, otros dentro de la parte del sistema operativo. En este momento, vemos que ISP se están haciendo mucho y con el tiempo están acercándose más a los sistemas operativos. A medida que va pasando el tiempo, iremos viendo más cambios en esto.

DAVID MORISON: Soy David Morison de Nueva Zelanda para el registro. Tenemos DNSSEC y estamos trabajando. Trabajo mucho con los registradores. Tenemos 4% de DNSSEC ya. Obviamente, tiene buenas razones para implementarse para el bien del público. Hablé con Rich Trust **01:03:03** sobre la demanda y la implementación. Me interesa saber el tipo de cosas que se pueden hacer para ayudar a educar a la población en general, para agregar más al lado de la demanda, para que se puedan entender los beneficios de la adopción de DNSSEC.

DAN YORK: Lo respondo yo, porque estoy muy interesado en implementarlo y en trabajar con eso. En el último año, en el desarrollo de este programa del que participo, tienes razón, hay una situación de la gallina y el huevo, donde tenemos que lograr la demanda y tenemos este problema constantemente. La gente se pregunta ¿para qué hacerlo si no hay tanta demanda? Por otro lado, hay otra gente que dice “por qué tengo que firmar mi zona si no hay tantos resolutores, como decía mi colega Gee.

Un paso importante fue el apoyo de Google; entonces, la gente empezó a pensar que quizás sería importante, a raíz de lo que consideró Google. Lo he visto en el tráfico y en las preguntas que hemos visto. Algo que se escucha en el taller del miércoles vamos a hablar de este tema "Casos de uso y distintas situaciones". Tenemos el mecanismo de Dane, de actualización del certificado utilizado con una capa adicional de integridad a nivel de certificado SSL, que sea el que la gente tiene que usar. Y agregamos una capa adicional de confianza con DNSSEC. Estamos empezando a ver algunos factores impulsores desde el punto de vista de los negocios que explican la razón por la cual hacerlo, con la gente que está acá en la mesa y con otros, todos trabajamos en maneras de ayudar a incrementar la demanda: CEO, CTO, CIO, a nivel ingeniería, con tutoriales para ver cómo funcionan las herramientas. Se ha simplificado mucho, ha mejorado mucho, hay un archivo de configuración que nos permite trabajar y era mucho más complejo. Todo está automatizándose, simplificándose y estamos transmitiendo el mensaje de la importancia que tiene. O sea, esto se viene.

RUSS MUNDY: Tenemos que seguirnos preguntando y tenemos mucha gente que participó, tratando de ayudar a generar la demanda. Honestamente, esa es una de las razones por las cuales comenzamos esta sesión, para que la gente entienda para qué sirve. Entonces podemos lograr el humo azul y podemos separarlo del humo negro. Esto es algo importante si seguimos trabajando para gente y explicándolo de esta manera, para la gente que no sabe de qué se trata el DNSSEC, se va a ayudar a que la

gente reconozca la importancia y aseguramos las actividades de internet.

SPEAKER: Quería mencionar que la República Checa ha tenido mucho éxito en su adopción. Ustedes deben querer hablar con Andre, asumo que está aquí.

RUSS MUNDY: Ellos están aquí; SIDN ha hecho un maravilloso trabajo en los Países Bajos, Suecia, también han trabajado muy bien este tema. En estos casos, si se fijan en lo que pasó, trabajaron de ambos lados. En República Checa, en Suecia, en los Países Bajos hay muchos ISPs que están haciendo validación y están incrementando la cantidad de firmas.

JULIE HEDLUND: Hay una lista acá.

QUESTION: Gracias. Soy …<**01:07:37**> de CNic. Mi pregunta es CNic ha decidido utilizar DNSSEC en un futuro no muy lejano. Quizás me podrían asesorar sobre cómo equivocarnos menos cuando implementemos DNSSEC en las primeras etapas, en el proceso al inicio de la operación.

JACQUES LATOUR: Está hablando de validación para generar archivos propios haya una seguridad de que están correctos. En punto.cr dedicamos mucho tiempo a desarrollar una solución. Tenemos lecciones en base al desarrollo realizado con los ccTLDs, con una especificación funcional de cómo hacer DNSSEC para verificar que esté bien hecho. Hay mucha tecnología de firmas, con varias alternativas y lo que elaboramos nosotros fue [ahí tiene un nombre errado] "Tecnología dual online signer", lo que quiere decir "firmamos más zonas con dos softwares distintos de DNSSEC y validamos el resultado para verificar que ninguno de los dos software se haya equivocado, en los cuales todavía no confío. Si uno valida contra las posibilidades de tener el mismo problema con distintos software a la vez, las posibilidades son bajas. En línea podemos verdad el material de Toronto. Y hay una presentación con la arquitectura de nuestra solución. Básicamente, hace falta dedicar mucho tiempo a verificar que esté bien firmado y la validación. Tenemos unas 16 pruebas después de generar el archive de zona para verificar que las firmas son válidas, que no vencieron, que no se eliminó ningún registro por error. Estuvimos 6 meses con preguntas y respuestas y encontramos bugs en DNSSEC abierto que no había descubierto otra gente, por la manera en que lo hacíamos. Así que podemos hablar en mayor detalle fuera de aquí si así lo desean, pero hay que dedicar tiempo a la validación del producto antes de publicar.

RUSS MUNDY: Sugeriría algo que Jacques no mencionó. La maquinaria que van a utilizar para hacer la validación de lo que produce el mecanismo de firma, también tiene que tener algunas zonas de prueba contra el

validador que intencionalmente puso información mala para verificar que el validador identifica todas estas cosas como fallas, de manera apropiada. En primer lugar, hay que verificar que el validador funciona bien y eso se hace poniendo datos que se sepa que están mal. Hay distintas herramientas para generarlos y el validador, uno puede verificar que está funcionando de manera adecuada. Las pruebas rigurosas constituyen el mensaje principal y la planificación de las contingencias.

QUESTION: Soy Deyham <**01:11:24**> de Yemen. Yo estudio y comencé a implementar la tecnología de circunvención de filtrado. Un área que me interesa es comprender la detección de los encabezados del tráfico, cuando empieza con el "handshake", el encabezado normalmente es plano, esta es un área en la cual pienso que hay una vulnerabilidad específica de DNS. ¿Han pensado encriptar los paquetes enviados o los encabezados o cabeceras para maximizar el potencial de evitar el abuso de las normas o estándares disponibles, junto con la curva de DNS, el protocolo introducido, etc.?

[Tenemos a alguien en el piso que puede hablar]

OLAF KOLKMAN: Solía dirigir el grupo de trabajo cuando se normalizó DNSSEC. Uno está solicitando privacidad en realidad, es un requerimiento muy puntual. Decidimos no trabajar en ello, porque los datos de DNS son públicos y

transmitidos en una alternativa transparente para todos. Era un requerimiento no específico el mecanismo de privacidad del protocolo que solo ofrece la autenticidad y la integridad, son los únicos controles que suministra. Es un no requerimiento realmente.

RUSS MUNDY: Puedo agregar que uno puede proteger la última comunicación. Hay tecnologías que se pueden utilizar para asegurar la conexión entre el resolutor y el sistema local.

DASHA VLADIMIR: Mi nombre es Dasha Vladimir de Rusia. Una pregunta sobre la implementación de punto.ru. ¿Cuál es su impresión sobre lo exitoso que fue esto, lo oneroso, el tiempo que llevó la implementación del estado de DNSSEC para hoy? Y sé que China está en un estado experimental. ¿Qué quiere decir y cuánto tiempo le lleva para implementarlo? ¿Puede compararlos?

RUSS MUNDY: No sé cuál es toda la historia de China, pero hace tiempo que está en experimento, porque está probando distintas cosas, pero el miércoles va a haber una presentación muy puntual respecto de los planes. Hay una diapositiva en la que van a hablar muy específicamente respecto de los planes que están por venir y seguramente puede hablar con la persona que está aquí adelante sobre ese tema. En cuanto a lo que hagan con eso, pero sobre el mapa puntualmente, hay distintas

graduaciones y estados y varía. Esto tiene que ver con lo que decíamos al principio, la complejidad, el tiempo involucrado, todo esto va a estar cambiando. Jacques habló de la cantidad de controles de calidad y garantía de calidad involucrada. Es difícil comparar manzanas y peras, por el equipo, por las partes, políticas, procedimientos, no se puede hacer una comparación sencilla por lo que existe.

JACQUES LATOUR: Nos llevó un año firmar punto.ca y cero.ca lo hicimos en unos minutos.

DAN YORK: No sé los detalles sobre punto.ru [contestan de la mesa ante una pregunta de la sala que no usó micrófono]. Creo que fue firmado recientemente.

RUSS MUNDY: Estoy familiarizado con el mapa y la metodología de recopilación de información y también trabajamos junto con John **01:15:38** de Chinkara, estrechamente en ese proyecto. Los datos recopilados son de carácter voluntario y se le pregunta a la gente en qué estadio está tu trabajo. Y son parámetros descriptivos generales. Los detalles del tiempo que le lleva a cualquiera en un estadio particular, dependen totalmente de esa organización y en la medida de la recolección de información, se pregunta cuándo van a poder migrar a la etapa siguiente. A veces la gente lo dice, a veces no. Como decía Dan, es un tema de peras y manzanas, aunque tengamos el mismo color en el mapa, son cosas

independientes y separadas, por lo cual es difícil hacer cualquier tipo de comparación cuantitativa.

DAN YORK: Con la excepción de que cuando están en el área verde, podemos validar, ya que sabemos que están los registros en la raíz y están publicados. No le puedo dar mejor información sobre eso.

QUESTION: Soy Bahar Doman <**01:16:56**> de Palestina. Quisiera preguntar sobre el tiempo de firmas, ¿cómo podemos medirlo?

DAN YORK: Entonces, la vida de las firmas. Bien, dentro de cada firma hay una fecha de vencimiento que está en la firma en sí. Así que tenemos que ir a la política de recomendación. Esos son datos publicados con las mejores prácticas que existen y varía. A veces se publica y tenemos diferentes claves y diferentes cosas. Los datos de la zona son válidos por un mes a tres meses y otras partes de las claves tienen una validez de un año. Varía, hay un documento que le podemos enviar con recomendaciones, se llama DNSSEC Operational Guidelines - Versión 2, sí, esta es la versión. RFC 6781 es el número del documento con esa información.

RUSS MUNDY: Y estas son recomendaciones, no son requisitos, sino que es un excelente lugar para comenzar.

JULIE HEDLUND: Tenemos otra pregunta en la sala.

NICHOLAS: Soy Nicholas, estoy en el programa de becarios. Me pregunto por el algoritmo de encriptación que se usa para los saludos o las diferentes partes del gamal Diffie Hellman y handshake ¿Hay un algoritmo o logaritmo o factorización?

DAN YORK: Podemos descender, hay diferentes algoritmos que están permitidos y definimos cinco o seis. Es una criptografía de clave pública. Hay muchos, no sé cuántos, no me acuerdo de memoria, pero hay variaciones. Hay un GHOST, hay un RSA, GHOST DSA, SHA1 y SHA3, SA1 y 256. Esto está ya en los documentos publicados. En las RSE.

WARREN KUMARI: Y también está diseñado para agregar otros protocolos a lo largo del tiempo.

SPEAKER: Bien, escuché que decían Diffie-Hellman y handshake; no hay nada de eso, no se trata de eso.

DAN YORK: Quisiera aclarar, porque yo hago la firma, yo comunico cuáles son los parámetros que utilizo para la firma y espero que el cliente valide. No hay handshake, no hay saludo. No es que pueda tomar estos argumentos y tenerlos.

RUSS MUNDY: En cuanto a la firma, dentro del DNS es el campo del algoritmo utilizado que está especificado para que los validadores puedan saber cuáles. Hay personas trabajando en este tema en una criptografía de curva elíptica y eso es otro algoritmo que va a estar agregado. Es extensible.

THOMAS: Soy Thomas, de un registro alemán, para las estructuras de clave pública y privada ¿quién está a cargo de la clave de raíz pública y si hay algún problema con ello, y si pasa eso, todo el DNSSEC en su proceso se rompe y quien está a cargo de esto?

RUSS MUNDY: La respuesta es hay un enfoque con mucha documentación, un buen enfoque que describe todos estos temas. La ICANN es fundamentalmente es la entidad encargada de la zona de raíz y sus

claves de firma, pero muchas personas de la comunidad que tienen que estar presentes cuando algo se hace con respecto a la clave de raíz en cuanto a protección de hardware y protección física que haya redundancia, esto está todo documentado y ustedes pueden ir en línea y ver los archivos de la actividad de firma de la clave. Julie Hedlund tuvo un papel principal en el mecanismo de la ICANN que ayuda a que no haya ningún problema.

SPEAKER: La pregunta es ¿esto es un punto de falla y puede fallar, esa llave puede tener algún problema y habría así un problema?

WARREN KUMARI: Hay una preocupación de que la clave pueda estar destruida. Hay sismos o, por ejemplo, algún problema por el estilo. Pero hay mucha discusión en vías sobre cómo hacemos y cómo desplegamos la clave de raíz. La RFC-5011 es una de ellas, pero no fue probado en la práctica este tema. Entonces, en teoría, mucha gente se une, genera una clave y una vez que se firma una clave se pasa la otra, pero no fue probado en el mundo real. Y sería importante saber cuándo desplegar la llave cuando hay algún problema, debería haber alguna política. Creo que hay alguna discusión sobre la clave de raíz.

DAN YORK: Yo iba a mencionar estos dos aspectos. Primero, la respuesta. El documento se refiere a que si se hace una búsqueda de “DNSSEC policy

and practice statement" o DPS, estos son los documentos que existen y están disponibles y muchos de los TLDs que están firmados, tienen sus propios DPS, que dicen qué es lo que está pasando, pero el de la raíz está muy involucrado y creo que root.dnssec.org me podrían informar con mayor precisión. Y esto los digo a todos los que están y quieren saber cómo firmar sus propios ccTLDs, u otros. Vayan a las prácticas de DNSSEC, porque ahí se describen cómo diferentes organizaciones lo hacen. En las consultas, la ICANN tiene comentario público que termina este viernes, el 12 de este mes, y esperan obtener feedback, porque esto se refiere a las mejores prácticas. Nosotros tenemos dos claves, las claves de la zona para firmar todos los datos actuales y también puede tener un nivel más alto de protección criptográfico. Las claves de la zona raíz cambian todo el tiempo, pero la última de las claves ICANN tiene un contrato que tiene que desplegarla en los primeros cinco años y esta es la zona que está en discusión, porque tiene que ser hecho antes del 2015 según contrato, así que la ICANN quiere tener las opiniones que ustedes puedan dar. Esto figura en la página de la ICANN. Muchas gracias.

JULIE HEDLUND: Bueno, en la sesión del miércoles va a estar Joe de ICANN y Yab Ackerhaus de Security and Stability Advisory que van a estar hablando sobre este tema. ISAC está considerando el tema también. Y están pensando qué decir, así que están invitados a unirse al debate. Va a ser muy interesante. Así que esperamos escuchar la opinión de ustedes. Y estamos ya retrasados unos minutos, así que quisiera que, ya que tengo

el micrófono ¿hay alguna última pregunta antes de cerrar esta sesión? Bien, Russ te doy la palabra.

RUSS MUNDY: Muchas gracias a todos por las excelentes preguntas y la excelente interacción. Muchas gracias a todos. Y si ustedes necesitan más información sobre el DNSSEC, el miércoles en la mañana, vamos a comenzar a las 08:30, antes de la mayor cantidad de sesiones, porque tenemos mucha información, así que si ustedes tienen mayores preguntas u otras preguntas, están invitados.

JULIE HEDLUND: De todas maneras va a haber almuerzo, pero de todas maneras tienen que participaren la sesión. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]