KOBE – DNSSEC para todos: guía para principiantes
Domingo, 10 de marzo de 2019 – 15:15 a 16:45 JST
ICANN64 | Kobe, Japón

WES HARDAKER: Y tendremos que poner la pantalla, porque ahora tenemos la indicación de las actividades de ese DNSSEC. Ya lo vamos a resolver. Un segundo.

Hoy vamos a hablar acerca de qué es la DNSSEC y de qué forma protege el uso de internet de todos, y en qué medida participa la ICANN. Yo soy Wes, del USC Information Sciences Institute. Tenemos acá un equipo de actores fantástico, los voy a presentar en un minuto.

Mientras tanto, quisiera contarles una historia acerca de DNSSEC. ¿Cómo comenzó? Comenzó hace muchísimo tiempo, en el año 5000 A.C. en la época de los dinosaurios. Y comenzamos con Ogwina, que es nuestra protagonista de hoy. Vive en las cavernas, en el límite del Gran Cañón. Él es Og, vive en el otro extremo del gran cañón, también en una caverna. Están muy lejos, porque el Gran Cañón es muy profundo, y muy extenso. Y ellos no tienen la oportunidad de conversar con frecuencia porque están muy lejos.

En una de las muy poco frecuentes visitas cruzaron el canal, hablaron, y observaron que salía humo de la fogata de Og y pensaron: ‘‘Esta es una posibilidad, nos podemos comunicar utilizando señales de humo’’.

Y muy pronto comenzaron a conversar frecuentemente utilizando el humo, y todo funcionaba muy bien. Hasta que un día, el pícaro Kaminsky se mudó cerca de Og y empezó a enviar señales de humo al mismo tiempo. Ahora Ogwina está muy confundida porque recibe dos series de señales de humo y no sabe cuál es cuál.

Entonces, Ogwina baja del cañón y trata de entender que está pasando. Ogwina y Og consultan a los sabios del pueblo. El hombre de las cavernas, Diffie – quizás sepan quién es Diffie. Un criptógrafo famoso, que ayudó a desarrollar la tecnología de DNSSEC. Él va al fondo de la caverna de Og, donde encuentra un polvo mágico azul. Tiene un color extraño, va corriendo a la fogata, lo tira al fuego, y debido a que la fogata se convierte en una fogata azul, gracias a eso, Ogwina y Og ahora pueden continuar conversando, porque ella sabe que solo tiene que creerle a las señales de humo azules, porque el humo azul proviene solamente de la caverna de Og.

¿Sí? Esa fue toda la introducción a DNSSEC. Ya entendieron todo, ¿No? Bueno, vamos a explicarlo después en mayor detalle, pero

el concepto subyacente, el concepto de que algo mágico convierte algo que sabemos que proviene del lugar exacto, eso es DNSSEC.

Vamos a volver un poco atrás, y vamos a ver cuál es el concepto general de DNSSEC. Si fueron a la clase de DNS para principiantes hoy y ayer, seguramente habrán visto este diagrama. EL DNS comienza en la parte superior, en la raíz, es un tema que se habla mucho en ICANN. Y por debajo tenemos todos los TLD's, a veces hay códigos de país, a veces hay cosas como com. Gracias. Y por debajo tenemos los dominios de segundo nivel, como co.uk y bigbank.com y nic.ma. Hoy nos vamos a concentrar en bigbank.com.

Entonces, lo importante que tenemos que saber es que el ISP tiene un resolutor, y el resolutor sabe dónde está la zona raíz, y siempre y cuando sepa dónde está la zona raíz, puede seguir esta cadena hacia abajo para saber dónde está todo lo demás. Entonces, va por la raíz, luego va bajando y ahí llega a com, y va bajando, y después vamos a hablar acerca de este tema en mayor profundidad y vamos a ver un ejemplo. Pero, en cada nivel el resolutor es guiado hacia el siguiente nivel. Entonces, se responde la pregunta y el resolutor almacena esa memoria durante un tiempo. Almacena eso en la memoria.

El problema es que no hay seguridad en DNS. Cuando se inventó, no sé en qué año, hace mucho tiempo en el ’84, no se le agregó seguridad. Todos eran buenos en esa época, no había nadie malo. Y es muy fácil después hacer la usurpación y envenenar lo que está en la memoria cache. Entonces, no se recuerdan solamente las respuestas buenas, sino también las malas durante mucho tiempo.

Para ejemplificar esto a mayor detalle quisiera llamar a los personajes que tengo aquí. Estas personas van a mostrarles exactamente que hace un ISP y el resolutor. Vamos a empezar acá con Joe User. Él va a tener que hacer alguna transacción bancaria hoy en bigbank.com, entonces él va a hacer una transacción bancaria, y vamos a ver como el DNS lo lleva a, esperemos, la respuesta correcta.

RUSS MUNDY: Hola, ISP. Necesito hablar con bigbank.com. Acá está el nombre.

WES HARDAKER: Ah, no sé qué es bigbank.com. Lo voy a averiguar, enseguida vuelvo.

Hola, raíz. Quisiera llegar a www.bigbank.com. ¿Podrías decirme qué es eso?

HOMBRE SIN IDENTIFICAR: Hola, yo soy el servidor de la zona raíz, yo conozco los dominios de alto nivel, ¿Usted busca a .com? ¿Por qué no va al servidor de .com en 1.1.1.1?

WES HARDAKER: Ah, perfecto, voy a ir. Hola, .com. Estoy buscando a www.bigbank.com, ¿podrías decirme dónde está?

HOMBRE SIN IDENTIFICAR: No sé dónde está www, pero puedo decirle donde está bigbank.com. Está en 2.2.2.2.

WES HARDAKER: Hola, ¿qué tal? Estoy tratando de llegar a www.bigbank.com. ¿Podría decirme donde lo encuentro?

RUSS MUNDY: Sí, yo se lo puedo decir, porque yo soy bigbank.com, y yo sé dónde está www.bigbank.com, está en 2.2.2.3.

WES HARDAKER: Fantástico. Voy a ir a ver a mi usuario.

RUSS MUNDY: Y quizás quiera darle este dinero.

WES HARDAKER: Hola, aparentemente usted se conectó con 2.2.2.3. Ahí está bigbank.com.

HOMBRE SIN IDENTIFICAR: Gracias, bigbank.com.

WES HARDAKER: Muy bien, gracias a estos tontos actores, les agradecemos su trabajo. Sí, sí, vamos a aplaudirlos. Pero esperen, porque esto mejora más aún. Toda esta actuación es muy parecida a la forma en que Ogwina se comunica con Og a través del resolutor.

La pregunta es, ¿qué pasa con el malo de Kaminsky? Que genera una señal de humo equívoca. ¿Cómo surgen los problemas? Ahora vamos a ver exactamente la misma obra. Va a ser exactamente lo mismo, van a ver, se los prometo.

RUSS MUNDY: Hola, ISP.

WES HARDAKER: ¿Qué tal?

RUSS MUNDY: Necesito hacer un depósito en bigbank.com. ¿Podría por favor buscar a esta persona?

WES HARDAKER: Claro, ningún problema. www.bigbank.com. Le voy a preguntar a la raíz.

Hola, raíz. Uno de mis usuarios quiere llegar a bigbank.com. ¿Podrías decirme donde lo encuentro?

HOMBRE SIN IDENTIFICAR: Puedo decirle que hable con el servidor .com en 1.1.1.1.

WES HARDAKER: Perfecto, le voy a preguntar a él. Hola, servidores .com. Uno de mis usuarios quiere contactarse con bigbank.com. ¿Dónde está?

HOMBRE SIN IDENTIFICAR: No sé dónde está www, pero puedo decirle donde está bigbank.com. Está en 2.2.2.

WES HARDAKER: Fantástico. Voy a preguntarle a él. Hola, uno de mis usuarios quiere conectarse con www.bigbank.com, ¿podría decirme dónde está?

HOMBRE SIN IDENTIFICAR: Sí. Seguro, no hay problema, bigbank.com está en 6.6.6.

WES HARDAKER: Bueno, gracias. Hola, usuario, usted debería conectarse con 6.6.6.6. Ahí se va a encontrar con bigbank.com.

RUSS MUNDY: Perfecto.

HOMBRE SIN IDENTIFICAR: Yo voy a tomar este depósito, señor. Muchas gracias.

WES HARDAKER: Ya ven cual es el problema. El pobre no sabe a quién creerle. Él le cree a la primera respuesta que recibe. Este es el tema con las señales de humo. Hay dos señales y el usuario tiende a creerle a una de ellas. En este caso, Ogwina no sabe cuáles son las señales de humo a las que le tiene que creer.

Volvemos a nuestro concepto general de DNS. Antes hablábamos acerca de la raíz que estaba arriba, los com que

estaban abajo, y después bigbank.com, y si uno está comunicándose, o si el resolutor en el ISP está hablando con el sistema equivocado, quizás obtenga una respuesta buena, la azul, o una mala, la roja.

El DNSSEC corrige esto, resuelve esto. Le agrega, le incorpora seguridad al DNS. Seguridad que antes no existía. Y lo hace mediante firmas digitales. Hay dos puntos importantes, por un lado dice que la información no ha sido alterada en ningún momento a lo largo de la trasferencia, y también dice que se originó en el lugar correcto. Podemos saber que se originó en el lugar original correcto, aun si estaba almacenado en el fondo de algo. Si fue firmado es válido para siempre. Las claves y firmas se almacenan en el DNS, lo cual es muy bueno porque para saber si el usuario está en un sitio seguro podemos usar el DNS para que haga las búsquedas, y nos diga cuales son las claves que necesitamos, y después vamos a ver un ejemplo.

Así como el resolutor antes solo tenía que saber dónde estaba el servidor raíz, para empezar ahí, y luego ir hacia abajo, con DNSSEC ocurre lo mismo. El resolutor solo tiene que saber dónde están los servidores raíz, y tienen que saber una clave de la raíz, y luego pueden continuar con la cadena, ya que cada nivel firma la clave siguiente. Si uno sigue esa cadena criptográfica hacia abajo sabrá que está recibiendo las respuestas correctas.

Ahora, entonces, volvemos a este diagrama que vimos antes. A veces no sabemos si creerle al azul o al rojo, pero ahora de esta forma sabemos que el rojo no va a funcionar. Vamos a ver qué ocurre en nuestra obra de teatro. Vamos a ver si podemos hacerlo con el bien y no con el mal.

¿Será posible? Sí, es posible.

RUSS MUNDY: Hola, ISP. Necesito comunicarme con bigbank.com, y necesito saber que estoy recibiendo una repuesta válida.

WES HARDAKER: Muy bien, voy a averiguarlo. Hola, raíz. Uno de mis usuarios quiere hablar con bigbank.com. ¿Podrías decirme por favor dónde está?

HOMBRE SIN IDENTIFICAR: Sí, puedo decirle donde está .com, 1.1.1, y acá puede ver la certificación que demuestra que la información que le estoy dando es correcta.

WES HARDAKER: Muy bien, fantástico, voy a confiar en usted. Voy a preguntarle al servidor .com.

Hola, ¿qué tal? Uno de mis usuarios quiere hablar con bigbank.com. ¿Podría decirme por favor dónde está? Y yo voy a verificar su firma cuando me dé una respuesta.

HOMBRE SIN IDENTIFICAR: Por supuesto, no puedo decirle donde está bigbank.com... en 2.2.2.2. Sí, está ahí.

WES HARDAKER: Hola, ¿qué tal? Yo quisiera saber cuál es la dirección de bigbank.com. ¿Me podría decir, por favor, dónde está?

HOMBRE SIN IDENTIFICAR: bigbank.com está en 6.6.6.6.

WES HARDAKER: Muy bien. A ver, un segundito, acá esto no coincide, no está firmado.

HOMBRE SIN IDENTIFICAR: Eh, yo no tengo...

WES HARDAKER: No, le voy a preguntar a otro. No confío en usted.

Hola, ¿podría decirme, por favor, donde está www.bigbank.com?

RUSS MUNDY: Sí, yo sé, bigbank.com está en 2.2.2.3, y acá puede ver la firma.

WES HARDAKER: Oh, me parece que es válido. Hola, Sr. Usuario, bigbank.com está en 2.2.2.3. Yo verifiqué la firma y usted puede confiar en esta información.

RUSS MUNDY: Yo acá veo la firma y se lo agradezco. Gracias, big bank.

WES HARDAKER: Muchas gracias. Un aplauso para los actores, por favor. Hicieron un muy buen trabajo. Si van a otras reuniones de ICANN en el futuro, hacemos esto todas las veces. ¿Alguno de ustedes ya vio esta obrita? Levanten la mano. Un par de personas ya la vieron.

Entonces, esto es equivalente al humo azul. Ogwina finalmente puede ver el humo azul. En esta obrita usamos unas claves colgadas del cuello de las personas, pero la idea es utilizar esta clave. Ahora le voy a dar la palabra a mi socio en este trabajo, quién va a hablar y les va a dar algunos ejemplos para explicarles por qué necesitamos DNSSEC.

RUSS MUNDY: Gracias, Wes. Yo soy Russ Mundy, de Parsons. Yo voy a tratar de ayudarles a entender mejor esto. A entender las cosas que tienen que pensar y analizar a lo largo del proceso.

Uno de los aspectos importantes del DNS es que muchas veces las personas, a veces olvidan que el DNS es utilizado por todas las aplicaciones que utilizan internet en la actualidad. Y si todo lo que pasa con el DNS no se hace correctamente, o hay un problema con la cadena, o si hay un problema que se da, son las aplicaciones las que sufren las consecuencias. O no nos podemos conectar, o en el caso de la obra que vimos el usuario no se puede comunicar con su banco. Entonces, eso es lo que pasa, y eso tiene que ver con lo que es DNS y lo que hace DNS.

Entonces, así como es fundamental que todas las aplicaciones funcionen, habría que preguntarse por qué las personas quieren atacar el DNS. Yo he estado viendo lo que pasa con el DNS, las actividades de seguridad de DNS durante muchísimos años, y honestamente nunca vi ni escuché ningún ejemplo donde se atacara el DNS simplemente porque lo quieren cambiar y nada más. No es así, no es lo que buscan.

Lo que buscan los que atacan el DNS es lograr acceso a información que está en algunas aplicaciones que envían consultas al DNS. Quizás simplemente quieran copiar el corro electrónico que viene de un sitio determinado, y quieren conocer

las direcciones hacia donde manda correos ese servidor de correo electrónico, y quieren quizás conseguir la dirección para los ataques de hombre en el medio, quieren recibir todos los correos electrónicos que hay en el servidor, y de paso quieren mandarlo a otro lugar y las personas que reciben el correo electrónico que ha sido modificado nunca se enteran. Son los ataques del hombre en el medio

Hace un par de años traté de ver si encontraba estos cursos que ya no están disponibles en internet, pero había uno o dos cursos donde los instructores en el plan de estudios exigían que los estudiantes escribieran un ataque de secuestro de DNS. Yo pensé ‘‘Esto no es bueno, esto está muy mal’’. Pero, también había paquetes de software en el mercado que nos permitían hacer lo mismo. Entonces, es muy fácil identificar herramientas o software que ya están circulando.

Y ¿en qué nos ayuda el DNS? Como ustedes vieron en la obra de teatro, la pregunta que planteó el usuario pasó por un proceso de verificación para verificar la exactitud del origen de la información y los detalles del contenido para ver que no se cambiaran en el transcurso de toda esa cadena.

Este es un ejemplo de los secuestros, es un ejemplo simplificado. No tan simplificado como en la obra que vimos, pero vamos a verlo. Fíjense, allí está la primera consulta, esa línea punteada,

se inicia con Joe User, el Usuario Juan. Después va al servidor, vuelve al servidor recursivo con la respuesta, y eso vuelve al usuario. Después, finalmente, después de que pasó todo esto, la consulta va al servidor web. Así que pueden ver que hay tráfico de red que tiene lugar, en el que muchas personas ni piensan. Ese es el tráfico de DNS que se da antes de que veamos el tráfico de servidor, o el servidor de Facebook, u otro tipo de tráfico.

Lo que hicimos hace un par de años fue crear un sitio especial para verificar que las consultas que se reciben sean validadas por el DNS y verificadas. Entonces, lo que hicimos fue lo siguiente: Hagamos una tilde, de aceptación, y eso me muestra que se hizo una verificación, después sí se plantea nuevamente la misma consulta y si no se estuviera utilizando DNSSEC, verían que esto no ha sido verificado por DNSSEC.

Después hicimos un secuestro de DNS que demostraría lo que podría suceder. Entonces, sale en la primera consulta el Dr. Malvado, nuestro asistente que estuvo aquí, el que tenía la capa negra, entra y da una respuesta y esa respuesta mandó al usuario Juan a un sitio web diferente. La consulta y la respuesta legítimas pasaron por el sistema pero el usuario Juan nunca las recibió porque la primera respuesta que recibió, que fue originada por el secuestrador, llegó a su equipo, y su equipo dijo ‘‘Muy bien, ya tengo una respuesta. No voy a seguir buscando’’.

Entonces, con DNSSEC, tenemos el mismo flujo de paquetes que ven acá. Pero la diferencia es que con la validación, con esta tilde de verificación, los paquetes que se reciben en las respuestas de DNS, que se reciben en las respuestas de DNS que vienen del secuestrador, no son aceptadas por el equipo de Juan, del Usuario Juan.

Los paquetes siguen moviéndose y avanzando. ¿Cómo es el sitio web personalizado? Este sitio web es muy parecido al que vimos antes. Nosotros hicimos un secuestro, y en este caso esto lo hicimos cuando Steve Crocker era presidente de la junta directiva de la ICANN, por eso lo tenemos allí, y él estuvo trabajando con el DNSSEC por mucho tiempo así que incluimos un link humorístico en otro lugar, que iba completando una parte de la pantalla que veía el usuario si llegaba a este sitio sin hacer la verificación a través de DNSSEC. O sea, secuestramos de hecho nuestra propia información en este caso, simplemente para ejemplificar que podría pasar si hubiera un ataque dirigido a una página como esa.

Cuando empezamos con el resolutor vacío y el navegador vacío, y después vamos a CNN.doc, hace 10 años veíamos esto. Y en la actualidad hay muchísimo material, se parece más bien a esto. Aquí simplemente vemos lo que se necesita para llenar una página web, y lo importante en todo esto y la razón por la que hay que hacer DNSSEC es asegurarnos de que los datos de la

zona DNS, el contenido de la zona sea correcto y siga siendo correcto mientras avanza y atraviesa la internet.

Entonces, otro ejemplo muy simple: esto es una zona no firmada, y al hacer la consulta, aquí vemos que pasa con la respuesta en la serie de pasos, y esto funciona en el trasfondo y después cuando agregamos DNSSEC, ya sea que estemos operando el resolutor y haciendo la validación, si es un ISP o una empresa, una organización local, ya sea que estamos haciendo una operación de un servidor de nombres. Quizás seamos un registrador y trabajemos con muchos servidores de nombre. Si ustedes ya pueden tener sus propios sistemas DNS, incorporar DNSSEC a esos sistemas debería ser bastante sencillo. El mayor desafío ha sido en general lograr software que soporte esto, que permita agregar las funcionalidades de DNSSEC. Pero esto ha mejorado mucho en los últimos años.

Entonces, las mayorías de las veces se pueden agregar DNSSEC si ya estamos operando en nuestro servidor de nombres. Solo se trata de utilizar el software correcto.

SI son organización de gran escala, como un TLD, o una empresa realmente muy grande, probablemente deberían hacer esto ustedes en lugar de tercerizarlo. Entonces, una vez más, es simplemente una ampliación de las funcionalidades que la organización seguramente ya tiene. Si son un usuario final,

entonces ustedes como personas individuales podrían pedir una validación de DNSSEC al proveedor de servicios de internet, ya sea una empresa o un ISP, y en ese caso seguramente ustedes no usarán su propio servidor de nombres.

Saben que algunas personas lo tienen, pero la mayoría de las veces es un tercero que lo opera para las personas individuales, y ese tercero debería hacer la validación de DNSSEC para impedir que el Dr. Malvado robe su información de DNS.

Como dije antes, hoy en día el objetivo principal de DNSSEC es asegurarse de que los datos de la zona, que son agregados al principio, ya sea por big bank, o .com, o por otra empresa, la idea es asegurarse de que esos datos se mantengan en el sistema y que vayan desde el sistema DNS al usuario final sin sufrir modificaciones en el recorrido. O sea, es el contenido de la zona lo que importa.

Y en ese debemos concentrarnos, en el contenido de la zona, para que este contenido llegue al lugar correcto y adecuado, y eso es muy importante. En algún momentos muchas personas realmente se concentraban y decían ‘en ese utiliza criptografía, y esto es algo muy especial, tenemos que hacer cosas muy especiales y difíciles’.

Deben asegurarse de que este sistema se maneje correctamente y las claves se manejen correctamente, pero el software

moderno generalmente lo logra. Lo que debemos recordar es que también debemos administrar el contenido correctamente, lograr que llegue sin modificaciones en el recorrido, que llegue hasta el servidor de nombres, y una vez que están allí hay que utilizar DNSSEC para validarlos.

Entonces, desde las imágenes que vimos al principio hasta aquí no vemos enormes diferencias, pero podemos ver que conceptualmente simplemente se están agregando algunos tipos de registros especiales en el sistema de DNS, que trabajan con la generación de la zona que está en el servidor autoritativo, después se trata de validarlos, y los servidores recursivos son los que validan la información; y esto es lo que vimos en la obra, cuando se pasaba de raíz, a com, a big bank.

En cuanto a DNSSEC, lo importante a tener en cuenta es en qué medida participa su organización en la operación del DNS actual. Si ustedes están operando el DNS actual y todos los servidores de nombres, y usándolos ustedes mismos, seguramente podrán prestar estas funciones adicionales que se necesitan para tener firmas y validación de DNSSEC en los lugares necesarios.

Ahora, si ustedes no están operando esto directamente muchas grandes empresas, por ejemplo, tercerizan la funcionalidad de DNS para su empresa. Por ejemplo, Parsons.com utiliza un proveedor externo por diversas razones, y una de las razones por

las cuales eligieron a este proveedor externo es que este proveedor utiliza DNSSEC. Si utilizan un proveedor externo deberían pedirle a este proveedor externo que brinde los servicios de DNSSEC, y no teman tampoco cambiar de proveedor si el actual les dice ‘‘Lo siento, pero yo no sabía que ustedes querían DNSSEC. No puedo prestarle este servicio’’. Busquen un proveedor que sí se los preste. Hay muchos que lo prestan.

Entonces, esta actividad es organizada en forma conjunta por la ICANN, el comité asesor de seguridad y estabilidad. También algunos miembros del comité asesor del sistema de servidores raíz que nos están ayudando hoy, y también a través del programa Deploy360 de la Internet Society. Estos grupos han estado apoyando estas actividades desde hace mucho tiempo, creo que esta ya es nuestra última diapositiva, y ahora llegó el momento de las preguntas.

WES HARDAKER: Muchas gracias, Russ. EL Dr. Malvado va a bajar para acercarles el micrófono. No sé si tienen alguna pregunta sobre lo que vimos o sobre algún tema que no se haya tratado, levanten la mano y Andrew les va a acercar... ¡Perdón! El Dr. Malvado se va a acercar y les va a dar el micrófono.

ANGELA: Hola, yo soy Ángela, de Botswana, de la autoridad reguladora de comunicaciones del país. En caso de que la clave pública fuera secuestrada, ¿hay algún mecanismo que se pueda implementar para decir, ‘‘bueno, si secuestran la clave’’, como podemos verificar si esto se corrige, o si el sistema manda las respuestas correctas?

WES HARDAKER: Eso es una pregunta muy buena, sorprendentemente buena. Muchas gracias, una muy buena pregunta. La pregunta sería, ¿qué pasa si se ve comprometida la clave?

Hay otros expertos aquí que también podrán, quizás, aportar en la respuesta. Hay dos claves involucradas aquí, hay una clave pública y una privada. Usted mencionó la clave pública, la pública se puede compartir con todas las personas. Es seguro, el objetivo de las claves públicas es que se puedan compartir. Las claves privadas son las que hay que proteger, si se ve comprometida esta clave privada, sí, inmediatamente hay que comunicárselo al nivel superior. Deben comunicarle al nivel superior que han cambiado esta clave privada si ha sido comprometida.

¿Vieron que se verificaron las medallas metálicas en esta obra de teatro? Bueno, habría que modificar esta medalla que tenía .com y decirle ‘‘Bueno, tengo una nueva clave, pues la clave privada

ha cambiado''. Y esto se puede cambiar rápidamente. Esto es muy complejo por supuesto, hay que trabajar con la memoria caché y ver qué pasa, etc, pero básicamente es lo que hay que hacer. Hay que decirle al nivel superior ''Tengo una nueva clave, y la vamos a cambiar ya. Esto los protege rápidamente.

¿Hay alguna otra pregunta? Fue una muy buena pregunta, gracias.

SAVYO VINICIUS DE MORAIS: Hola, yo soy Savyo de Brasil, soy NextGen. Mi pregunta es la siguiente: ¿Cuál es el mayor desafío que enfrentan ustedes en cuanto a DNSSEC? Para que DNSSEC sea utilizada por más usuarios.

WES HARDAKER: La pregunta es ¿Cuál es el desafío en cuanto a lograr que más usuarios utilicen DNSSEC? ¿Alguien quiere contestar esta pregunta? Russ.

RUSS MUNDY: Gracias. Esto ha sido un trabajo constante en cuanto a educar, en cuanto a alentar a las personas a usar esto a través de diferentes foros. Foros como este, por ejemplo. Y el trabajo que se ha hecho en diferentes actividades para trabajar con

proveedores de software, para ver que tengan la estructura y las funcionalidades adecuadas en su software, y también hemos trabajado con proveedores de aplicaciones para alentarlos también a utilizar DNSSEC.

Yo creo que una de las cosas que más nos ha ayudado para que más personas utilicen DNSSEC, es lo que hacen los usuarios. Ya sean personas individuales u organizaciones que dicen ‘‘yo quiero utilizar DNSSEC’’, algunas de las funcionalidades de registradores, algunas de las empresas no trabajan con DNSSEC, con lo cual es difícil que un usuario reciba esta validación.

La mayor parte de los operadores de registros si trabajan con DNSSEC correctamente en la actualidad. Pero en cuanto a los usuarios finales, bueno, estos usuarios también pueden pedirles a los proveedores de software que utilicen DNSSEC, y si aumenta la demanda y aumenta el volumen de la demanda, esto seguramente será la principal motivación que deben recibir los proveedores. Porque a lo largo del tiempo, a medida que diferentes programas han encarado directamente esas actividades, la respuesta la mayoría de las veces ha sido ‘‘nuestros clientes no lo están pidiendo’’.

Entonces, por eso, organizamos reuniones o sesiones como esta, para que no solamente se entienda qué es, sino para que

ustedes entiendan que ustedes como usuarios finales tienen un rol, y es pedir que se haga DNSSEC.

HOMBRE SIN IDENTIFICAR: Algunas diapositivas antes de la última diapositiva vimos un diagrama que tenía los resolutores de validación. Cuando medimos el éxito de DNSSEC, vimos cuantas zonas se firmaron, eso es una forma de medirlo, ¿pero hay algo que es sumamente importante cómo ver quien está validando? No sirve que tengamos todos los dominios del mundo firmados si las aplicaciones o si los resolutores recursivos no lo están utilizando. Y también quería decir algo más, pero no lo recuerdo, así que termino aquí.

WES HARDAKER: Buena pregunta, continuamente tratamos de obtener datos estadísticos y hacer un seguimiento para ver si el sistema está creciendo. A lo largo del tiempo DNSSEC ha continuado creciendo, no crece con la velocidad que nos gustaría, porque nunca llega a eso.

Esta es una página que yo creé, se llama stats.dnssec-tools.org. Los datos provienen de Víctor Duchovny que es un experto en este tema, y como podrán ver han habido grandes crecimientos recientemente, muy recientemente, en los últimos dos meses, y

vemos que los servidores de email utilizan los registros firmados del DNSSEC. Algunos datos provienen de empresas que comenzaron a llevar todos sus servicios de email a esto, y los activan todos al mismo tiempo, por eso vemos ese gran crecimiento.

La buena noticia es que cada vez se utiliza más, pero en gran parte es el boca en boca, en gran parte son actividades como estas, las actividades que realiza ISOC, pero todavía hay mucho por hacer. Creo que hay 10 millones de dominios firmados, pero la realidad es que hay muchísimos más, así que continuamente tratamos de crecer. ¿Hay alguna otra pregunta?

[COFY]: Estoy acá. Soy [Cofy], del registro de nombres de Ghana, y tengo dos preguntas breves. En primer lugar, quiero referirme a la primera pregunta que se hizo, ¿Es una buena práctica estándar tener claves privadas y cambiarlas periódicamente para que no se vean afectadas? Y la segunda pregunta es, ¿DNSSEC es un requerimiento para lograr la acreditación de la ICANN para los registradores y ese tipo de organizaciones?

WES HARDAKER: Es una buena pregunta. Para responder la primera pregunta hay dos corrientes diferentes, algunos consideran que no hace falta

ir rotando las claves hasta que una clave no se ve afectada, porque si la clave es lo suficientemente fuerte... podemos tener clave débil, pero si es lo suficientemente fuerte no hace falta cambiarla. Yo no cambio mis claves con tanta frecuencia.

La guía general es que si no lo hacemos no vamos a saber cómo hacerlo, entonces, desde el punto de vista operativo si uno lo hace paródicamente uno puede asegurarse tener las habilidades necesarias para poder hacerlo en caso de que sea necesario. Muchas personas van cambiando sus claves periódicamente una vez por año o algo así.

Con respecto a la segunda pregunta, la ICANN tiene determinados requerimientos para algunos organismos con los cuales tiene contrato. Por ejemplo, todos los nuevos gTLDs tienen que poder operar con DNSSEC. ¿Los nuevos registradores también tienen que tener DNSSEC?

RUSS MUNDY: No estoy seguro, pero me parece que no hay un requerimiento todavía estipulado para los registradores.

WES HARDAKER: Muy buena pregunta, gracias. Hay una pregunta acá, y hay dos al fondo.

[CORY]: Yo soy de Estados Unidos. Tengo una pregunta relacionada específicamente relacionada con estos temas. DNSSEC existe desde hace varios años, pero recientemente se ha hablado acerca de DNS sobre TLS o HTTP, entonces, ¿Cómo funcionan con DNSSEC? ¿Son complementarios, compiten, como se relacionan entre sí?

WES HARDAKER: Es una buena pregunta. Se ve que ustedes están muy bien informados sobre este tema. Hay un par de cosas, no compiten, son complementarios. Las DNSSEC firman los datos, no importa cómo se transportan o donde se mantienen almacenados, lo importante es saber que el registro no fue alterado. La DNSSEC sobre TLS es una especificación reciente que encripta y autentica el tráfico entre dos dispositivos. Y tenemos el DNS sobre HTTPS, que tiene una ventaja principal y es que no puede ser afectado por firewalls.

Hay diferentes razones para elegir alguna de estas tecnologías en particular, pero la diferencia más importante entre DNSSEC y los otros dos, es que DNSSEC lo firma en forma tal que no importa donde uno lo recibe, sabe que su integridad ha sido protegida. Si uno hace DNSSEC sobre TLS, o sobre HTTPS, uno

sabe que esa transacción está bien, pero no tiene la información histórica para saber cómo llegan esos datos ahí.

Entonces, DNS tiende a utilizar muchos grupos. Por ejemplo, uno puede hablar con los diferentes proveedores que lo hacen, pero no sabes qué es lo que pasó detrás de escena, y uno no sabe si tiene los datos correctos, si esos datos fueron verificados. Los servicios autoritativos no hacen DNS sobre TLS o sobre HTTPS. Buena pregunta.

RUSS MUNDY: Quiero agregar algo con respecto al taller del miércoles. El miércoles hay un taller sobre DNS, con una presentación específica en el taller acerca de ese tema exactamente.

WES HARDAKER: Sí. El miércoles es un gran día. Sí les interesa DNSSEC, el miércoles es EL día.

RUSS MUNDY: Quiero resumir brevemente lo que usted dijo, DNSSEC está para proteger los datos. DNS sobre protocolos encriptados apunta a proteger la privacidad de la consulta, y son dos cosas diferentes.

WES HARDAKER: La pregunta allí al fondo, y luego más al fondo.

[BALGISHNER]: Hola, yo soy de Nepal. DNSSEC protege al usuario final, ¿Hay alguna dificultad en cuanto a hacer que DNSSEC sea obligatorio? ¿Para qué todos utilicen DNSSEC?

WES HARDAKER: Es difícil, porque este es un mundo libre y la gente puede elegir utilizarlo o no. Hay una frase común que dice que no hay una policía de internet. No hay nadie que pueda diferenciar el bien del mal, o que pueda hacer cumplir o prevalecer el bien sobre el mal en el internet. Lamentablemente no hay ninguna forma de obligar a todos a que utilicen DNSSEC. Sería muchísimo más fácil, ¿No es cierto? Pero no es así.

RUSS MUNDY: Hay algunas organizaciones que sí decidieron implementar políticas de seguridad que obligan a utilizar determinadas tecnologías de seguridad. Entonces, algunas organizaciones decidieron hacerlo pero no hay una respuesta única para todos.

WES HARDAKER: Eso es un punto muy válido. Algunos gobiernos decidieron que toda la infraestructura del gobierno debe utilizar DNSSEC, que ese es un muy buen ejemplo. Gracias.

HOMBRE SIN IDENTIFICAR: Hola, soy [inaudible] de Sri Lanka. Y tengo una pregunta breve. DNSSEC interfiere en el flujo normal de DNS, quiero saber ¿qué es lo que hace?

WES HARDAKER: A usted le preocupa la velocidad que afecta DNSSEC. Es una pregunta excelente. Un par de puntos, por un lado DNSSEC es un poco más lento porque hace más solicitudes. Hay muchos estudios que muestran que hay gente que midió esto.

El punto más crítico es el siguiente: los datos de DNSSEC están en la memoria caché. Yo ya mencioné esto en la presentación, pero no lo mencionamos en detalle. Los aspectos de seguridad también están en la memoria caché, entonces una vez que uno encontró bigbank.com todos los registros tienen una fecha y dicen durante cuánto tiempo tienen que ser recordados. Entonces, eso queda en la memoria caché y eso está disponible durante un determinado tiempo.

Lo fantástico de DNSSEC es que la primera persona que hace la consulta, que es a principios del día quizás tenga una respuesta un poquito más lenta. Apenas un poco más lenta. Pero las siguientes consultas van a ser un poco más rápidas. Muy buena pregunta, gracias.

[CHRISTIANNE]: Hola, yo soy Christianne, soy de La Costa de Marfil, y quisiera saber los siguiente. Yo no soy especialista en la parte técnica, así que quizás mi pregunta les parezca tonta.

WES HARDAKER: No, adelante. Continúe.

[CHRISTIANNE]: Quisiera saber en el caso de un secuestro de DNS. ¿Hay una clase de procedimiento para que DNSSEC resuelva ese problema? ¿Hubo algunos casos en que se violaron esas instancias y hubo que actuar directamente?

WES HARDAKER: Usted acaba de mencionar un problema difícil. Hay muchas funcionalidades de seguridad en muchos protocolos y sistemas físicos que no están disponibles. La gente actúa cuando a veces ya es demasiado tarde.

Usted está preguntando lo siguiente: si alguien entró en su casa, si alguien le robó el dinero, ¿se puede hacer algo? Post-factos no. Se puede incorporar algo con anterioridad para evitar que ocurra algo. DNSSEC no puede resolver las cosas una vez que ya ocurrieron, una vez que ya ocurrió un secuestro. La buena

noticia es que así como la memoria caché con el tiempo se vence, esperamos que con el tiempo esa información se vaya y se empiece a utilizar la información correcta, pero si uno quiere proteger los datos de DNS hoy tiene que implementar DNSSEC antes de que ocurran estos problemas. ¿Entiende lo que digo? Gracias.

ABRAHAM: Yo soy Abraham, soy de Nigeria, y mi pregunta es lo siguiente. ¿Al implementar DNSSEC es necesario aumentar los requerimientos del sistema? ¿O mantenemos lo que tenemos antes de implementarlo?

WES HARDAKER: No sé si escuché correctamente porque hay mucho eco acá. ¿Usted quiere saber si hay un requerimiento adicional de hardware para implementar DNSSEC? Es decir, más CPUs, más memorias, ¿ese tipo de cosas? Sí. Perfecto.

RUSS MUNDY: Se hicieron diferentes análisis con respecto a este tema. En general, son análisis realizados por personas que se concentran en lo que ocurre a nivel de TLD o a nivel de la raíz. La conclusión rápida es que el crecimiento normal, en el ciclo de reemplazo de hardware que estamos siguiendo, alcanza.

Sin embargo, ¿cuáles son los números? Por lo que recuerdo el impacto sobre el hardware es de quizás un 3 al 8% en la firma. Pero eso no es en tiempo real, uno firma antes de cargar la zona. Para la validación está alrededor del mismo nivel, quizás llegue a un 10% incluso, no es un impacto muy importante pero sí es algo que debería ser tenido en cuenta especialmente cuando se considera el programa de actualización de hardware para la infraestructura de DNS.

WES HARDAKER: Gracias. Y también debemos saber que hay un aumento de la memoria porque hay más registros y ese tipo de cosas. Sí se necesita un poco más de memoria. Yo tengo unas 20 zonas, y nunca tuve que comprar más hardware para implementar DNSSEC en ninguna de las cosas que hice. Si ustedes son un TLD importante con muchísimos ingresos, entonces quizás sí tengan que considerarlo, pero la realidad es que probablemente para la mayoría de las personas esto no sea necesario.

[PAUL]: Soy Paul, del Reino Unido. ¿Hay algún mecanismo para hacer un seguimiento y monitorear las violaciones al DNS para los TLDs o los registradores?

WES HARDAKER: ¿Para monitorear con qué fin? Hoy escuchamos hablar de DNSSEC. ¿Usted se refiere al desempeño en términos de seguridad, o a los datos?

[PAUL]: Para construir una base de datos de las violaciones.

WES HARDAKER: Es muy difícil monitorear si se están utilizando mal las cosas o no, porque la realidad es que no se puede monitorear lo que hace todo el mundo. Yo puedo monitorear lo que hace el TLD, y ver si utilizan siempre la información correcta, pero en general los ataques no se producen allí sino más bien cerca del usuario final. Entonces, tendríamos que monitorear a todos los ISP del mundo. Es una pregunta muy compleja. Si quiere después acérquese a mí, si le interesa hablar en mayor detalle sobre este tema, porque es un problema difícil. Si tuviéramos la respuesta a esto ya habríamos dejado afuera todos los que quieren cometer un acto delictivo.

HOMBRE SIN IDENTIFICAR: Con respecto a los requerimientos de Hardware de DNSSEC, el centro de información de redes de la República Checa publica periódicamente benchmarks de los servidores con DNS y DNSSEC. Si quiere acérquese a mí después y le voy a mostrar

cual es el vínculo, para que vea cual es el impacto sobre el hardware, que realmente es mínimo. No van a notar nada al menos que reciban un millón de consultas por segundo en el mismo dispositivo.

WES HARDAKER: Muchas gracias. Hay una pregunta aquí.

[BRONWYN]: Hola, yo soy [Bronwyn] de Australia. Mi pregunta es la siguiente, ustedes en la obra de teatro antes mostraron que el resolutor pasaba la validación de certificado en cada uno de los niveles del dominio, ¿hay alguna actualización o algún cambio de software que sea necesario a nivel de resolutor para poder permitir esa validación adicional de forma tal que el resolutor pueda hacer resoluciones para los dominios con DNSSEC y sin DNSSEC?

WES HARDAKER: Es una muy buena pregunta. La mayoría de resolutores operan con DNSSEC; BIND probablemente sea uno de los más grandes, y es compatible con las funcionalidades más importantes de DNSSEC a lo largo de los últimos diez años. Es decir cualquier consulta reciente, incluso con la plataforma de un servidor de DNS, los resolutores de Windows también lo tienen. Cualquier cosa reciente seguramente no va a tener problema.

[CREJAN]: Hola, yo soy [Crejan]. Tengo dos preguntas. ¿Hay algún indicador que pueda considerarse para indicar que se necesita DNSSEC?

WES HARDAKER: Es una muy buena pregunta. Los ISP son los que necesitan implementar un validador. Ya vieron antes a mi amigo Warren que iba de persona en persona en la obra de teatro. Ellos son los que más tienen que trabajar, tienen que hablar con la raíz, con el TLD, con los servidores, tienen que hablar con ellos para todo, y ellos necesitan garantizar que su software pueda manejar las búsquedas seguras y no seguras. Porque la realidad es que hasta que todo el mundo no llegue a estar seguro, no podremos forzar la utilización de DNSSEC.

Hablamos de este tema antes, pero el DNSSEC nos dice: ‘‘Yo soy seguro, este otro servidor al que le estás haciendo una pregunta no es seguro, y yo puedo verificar y mostrarle que no es seguro. Así que usted debe asegurarse de estar seguro usted mismo’’. Queremos asegurarnos de que usted sepa en última instancia si está trabajando de manera segura o no.

El ISP puede monitorear los sitios, especialmente si hay problemas de validación o fallas de validación. Quizás haya un ataque, un problema en internet. Mirar los logs es una muy

buena forma de saber si usted está trabajando en una tecnología segura o no.

[ALFIFA]: Hola, yo soy Alfifa de Bangladesh. No sé si usted es la persona correcta para hacerle esta pregunta.

WES HARDAKER: Yo seguro que no. Es él.

[ALFIFA]: La pregunta es la siguiente. ¿Ustedes tuvieron algún incidente importante por el traspaso de la KSK?

WES HARDAKER: Esta es una pregunta que me va a servir para el taller DNSSEC. ¿Hubo algún problema después del traspaso de la llave? ¿Y qué hacen al respecto?

RUSS MUNDY: Gracias. Le pido disculpas, pero no escuché correctamente la pregunta porque la acústica es un poco difícil acá. El traspaso de la KSK no fue un evento que generó grandes problemas. Hay diferencias en cuanto al nivel de tráfico una vez que se revocó la clave anterior, pero el miércoles tendremos una sesión sobre

este tema y ahí les daremos información sobre ese tema. En realidad, desde el punto de vista operativo, no hubo un impacto identificable en el traspaso. Desde todo punto de vista fue un éxito operativo. Fue un gran éxito.

WES HARDAKER: Hay muchas presentaciones en talleres anteriores de DNSSSEC que explican porque se demoró el traspaso de la llave. Hubo muchas presentaciones sobre ese tema, yo también di varias presentaciones sobre ese tema, y el miércoles seguramente también tendremos la última presentación sobre este tema porque la fecha es el 11 de Enero, y ese fue el último paso del traspaso y hay datos interesantes que surgieron y que vale la pena analizar. Si les interesa este tema, acérquense a mí después y puedo enviarles también videos sobre este tema si es que realmente están tan aburridos.

¿Hay alguna otra pregunta? Nos queda algo de tiempo. No veo que nadie haya levantado la mano, así que muchas gracias por sus preguntas tan interesantes. Realmente ustedes son uno de los públicos más formados y con más conocimiento que hemos visto hasta ahora. No hay preguntas tontas, por favor. Siéntanse libres de acercarse más adelante si tienen otra pregunta. Lleva mucho tiempo aprender todo esto y nosotros hace 10, 20 o más años que estamos trabajando en este tema. Así que, no hay

preguntas tontas, solo hay preguntas de personas que están empezando a aprender sobre el tema.

Muchos de nosotros vamos a estar aquí todavía más tarde. Pueden acercarse a nosotros en cualquier momento. Disfruten el resto de la reunión de la ICANN, y por favor vengan al taller de DNSSEC el miércoles porque es un muy buen lugar para aprender sobre este tema. También vengan a participar del Tech Day el lunes. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]