HYDERABAD – DNSSEC para todos: introducción para principiantes
Viernes, 4 de noviembre de 2016 – 17:00 a 18:30 IST
ICANN57 | Hyderabad, India

WARREN KUMARI: Vamos a darle a la gente un par de minutos más para que ingresen en la sala y se sienten antes de comenzar.

Vamos a comenzar. Buenas tardes. Soy Warren Kumari. Esto es DNSSEC para todos. Habitualmente esto lo presenta Dan York y algunas otras personas. Pero lamentablemente, esta vez no pudieron venir. Mi laptop no tiene energía, no tiene conexiones, espero que funcione con la batería.

No sé cuántos de ustedes ya han estado aquí en esta sesión de DNSSEC para todos. Podrán reírse de todos una segunda vez cuando hagamos la parodia. Hay muchos que no la han visto así que va a haber muchos que se reirán.

Bien. La gente que sabe sobre DNSSEC sabrá que se inventó hace más de 10 o 15 años. Pero en realidad se equivocan, porque se inventó hace 7000 años, en la época de los hombres de las cavernas.

Esta es Ugwina. Ella vive en una cueva en el Gran Cañón. Y este es su novio, Ug, que también vive en una cueva en el Gran

Cañón. Lamentablemente el Gran Cañón es muy grande y lleva mucho tiempo cruzar de un lado al otro y mucho tiempo volver. Por eso Ugwina y Ug no se reúnen mucho, y eso los pone muy tristes. En una de las pocas veces en las que logran reunirse y conversar, se dan cuenta de que sale humo del fuego que hizo Ug, es entonces cuando se les ocurre una idea brillante. Si hacen señales de humo pueden conversar entre sí en uno y otro lado del Gran Cañón, y así no pierden tiempo cruzando y dando la vuelta. Pero un día otro cavernícola que se llama Kaminsky aparece en el lugar y por algún motivo quiere generar problemas, ¿y qué hace? Empieza a enviar sus propias señales de humo, y como Ugwina está lejos no puede distinguir quién está enviando las señales, entonces no sabe a qué conjunto de señales debe creer. Como le molestan algunas de las cosas que piensa que Ug le está diciendo, baja al cañón, trepa al otro lado y le empieza a gritar, y Ug le dice “pero si yo no dije esas cosas”. Entonces se da cuenta de que fue Kaminsky el que ha estado enviando señales falsas, y no saben qué hacer al respecto.

Van a ver a los sabios de la aldea y les piden ayuda, y uno de estos ancianos, que les dice que se llama Diffie, les dice que tiene una idea y entra a la cueva de Ug. Allí toma un puñado de la arena, que es muy especial, y lo que la hace especial es que sólo se encuentra en la cueva de Ug. Toma un puñado y la arroja al fuego, y las llamas se tornan de color azul. Ahora Ugwina

puede volver a su hogar y charlar con Ug porque sabe que lo único que tiene que leer es el humo azul e ignorar todo lo que no sea azul, porque no vendrá de Ug.

Y eso de alguna manera es lo que hace DNSSEC. Añade el color azul para saber cuál es el verdadero y cuál no lo es. Ahora le voy a dar la palabra a Wes. Vamos a hacer la introducción un poquito más lenta porque Wes tenía que estar en otro lugar, acaba de llegar. ¿Qué te parece si te sientas?

WES HARDAKER: Buenas tardes. Yo soy Wes. Vamos a continuar con una introducción del DNSSEC del DNS, luego del DNSSEC y después una parodia para que sea un poco más divertido. Bien. En primer lugar, el concepto de cómo funciona el DNS, que es como una estructura de árbol. De hecho lo llamamos un árbol, pero para mí es como un árbol que crece de arriba hacia abajo.

La raíz, que está arriba, es el lugar genérico donde todos tienen que ir. Si nadie sabe qué preguntar, hay que preguntar en la raíz. Por ejemplo, en bigbank.com, si no saben dónde comenzar, le preguntan a la raíz, "¿.com dónde está?". La raíz les dirá dónde está .com, no sabrá donde está bigbank, pero sí dónde está .com. Entonces bajamos un nivel. Un resolvedor, normalmente el ISP, es el responsable de manejar todas estas resoluciones. El teléfono, la tableta… normalmente no es la que maneja la

cadena, sino que se hace una pregunta al resolutor del ISP local y se le pregunta dónde está bigbank.com, y este sabe dónde disparar la jerarquía del DNS desde arriba hacia abajo para darles una respuesta.

Cada nivel refiere al resolvedor al siguiente nivel hasta pasar a quien hizo la pregunta. El resolutor guarda esa información en la calle durante un tiempo, entonces si ustedes vuelven a preguntar la respuesta surge más rápidamente. Y eso hace que también sea innecesario volver a preguntar a la raíz, porque está guardado en la caché.

El problema del DNS es que fue inventado en una época en que no había mucha seguridad en lo que es la esencia de Internet, porque no había demasiados actores, era todo gente que se conocía.

Pero ahora se falsifican muy fácilmente los nombres, aun cuando no sea la persona correcta la que conozca la información, puede envenenar o contaminar las cachés y modificar el contenido. Cuando hay una respuesta incorrecta en la caché se repite esa respuesta. Entonces el resolutor que tiene una mala respuesta la continúa alimentando porque la toma de la caché y es incorrecta.

Ahora vamos a hacer una parodia/juego y le voy a pedir a mis actores que se pongan de pie. Fíjense que están todos usando

unas lindísimas camisas o camisetas con sus roles. Si te pones tu camiseta sería fantástico. Y necesitamos los micrófonos volantes. Son distintos de los que vine usando esta semana. A ver.

¿Qué laptop controla las diapositivas? Porque tengo que apuntar.

ORADOR NO IDENTIFICADO: Hay una cosita que hace clic.

WES HARDAKER: Me encantan las cositas que hacen clic. Bueno, en la historia que Warren les acaba de contar, de Ug y Ugwina, Ugwina en realidad es la resolutora, es la que hace la pregunta: ¿dónde está Ug? Y Ug está donde sería el bigbank.com. Y Ugwina está confundida. Como vieron, puede haber dos versiones distintas de la respuesta que está recibiendo.

Comencemos con un caso muy sencillo. Vamos a tener al usuario Joe. Levanta la mano, Joe. Joe necesita hacer una transacción bancaria. Tiene que ir al banco y tiene que ir al lugar correcto. Va al banco y le dice, “Necesito hacer una extracción de dinero. Necesito hacer algunas transacciones, pagar cuentas.” Entonces tiene que hablar con un ISSP para obtener una respuesta. Ahí está el ISSP.

Cathy sería el servidor raíz. Ahí es donde todo empieza. Y también tenemos a .com y a bigbank.com para dar la respuesta. Y recuerden que, en definitiva, las computadoras hablan en números, con una dirección IPv4 o IPv6, y es responsabilidad de ellos traducir todos esos números para que puedan hablar.

Le paso la palabra a los actores.

ORADOR SIN IDENTIFICAR: Hola a todos. Soy el usuario Joe y hoy quiero hacer una transacción financiera en el banco y voy a escribir en mi navegador "www.bigbank.com". A ver qué pasa.

Quiero ir a www.bigbank.com

ORADOR SIN IDENTIFICAR: Yo no sé dónde está www.bigbank.com, a ver si lo encuentro. Hola Raíz, uno de mis usuarios quiere ir a www.bigbank.com ¿Me puede decir qué es?

ORADOR SIN IDENTIFICAR: No sé qué es pero sé dónde está .com. Pregúntale a .com

ORADOR SIN IDENTIFICAR: Hola .com, uno de mis usuarios quiere ir a www.bigbank.com, ¿dónde está?

ORADOR SIN IDENTIFICAR: Yo sé dónde está bigbank.com, está en 2.2.2.1.

ORADOR SIN IDENTIFICAR: Big Bank, quiero saber dónde está www.bigbank.com. Uno de mis usuarios quiere ir ahí.

ORADOR SIN IDENTIFICAR: Fantástico. Me encantan mis usuarios. Por favor, dile que vaya a 2.2.2.3.

ORADOR SIN IDENTIFICAR: Hola, usuario. Te encontré la respuesta, 2.2.2.3 es el lugar donde tienes que ir.

ORADOR SIN IDENTIFICAR: Perfecto. Ahora voy al navegador, hago mi transacción financiera y todo funciona.

WES HARDAKER: Excelente. Muchas gracias a todos. Vamos a hacer después otro caso más.

Eso fue fácil, ¿no? Así es como debería funcionar Internet. Todos responden con la verdad, no hay gente maliciosa, no hay malos actores. Todo funciona muy bien y Joe puede hacer su transacción perfectamente.

Lamentablemente, como dijimos antes, cualquiera puede falsificar las respuestas en el DNS. Una de las cosas que puede pasar, como vemos aquí abajo, en el recuadro de color rojo, es que alguien más responda donde está bigbank.com. Vamos a ver una segunda versión de la parodia donde uno de los malos entra a actuar. Vamos a ver qué pasa.

ORADOR SIN IDENTIFICAR: Muy bien. Lo mismo que antes. Quiero ir a mi banco, bigbank.com, para hacer una transacción y transferir 50 rupias de una cuenta. Quiero ir a esta dirección, a la cuenta de otro.

ORADOR SIN IDENTIFICAR: Yo no sé dónde está. A ver si encuentro la respuesta. Hola, Raíz. Uno de mis usuarios quiere ir a www.bigbank.com, ¿me dice dónde está?

ORADOR SIN IDENTIFICAR: No lo sé, pero puedo decirte dónde está .com.; .com está en 2.2.2.1

ORADOR SIN IDENTIFICAR: Hola .com, uno de mis usuarios quiere ir a www.bigbank.com, ¿dónde está?

ORADOR SIN IDENTIFICAR: No sé dónde está www.bigbank.com, pero sí sé dónde está bigbank.com. Está en 2.2.2.2.

ORADOR SIN IDENTIFICAR: Voy a probar con él. Hola, Big Bank. Uno de mis usuarios quiere llegar a www.bigbank.com, ¿dónde está?

ORADOR SIN IDENTIFICAR: Fantástico. Yo te puedo ayudar. Lo que tiene que hacer simplemente es ir a 6.6.6.6

ORADOR SIN IDENTIFICAR: Fantástico. Muy buena su ayuda. 6.6.6.6 es el sitio donde usted tiene que ir.

ORADOR SIN IDENTIFICAR: Perfecto. Entonces eso lo voy a poner en mi navegador y me conecto con el banco, a ver si por algún motivo mi cuenta bancaria tiene menos dinero, ¿qué pasó? Me parece que aquí hay un problema.

WES HARDAKER: Muy bueno el trabajo. Como ven – un aplauso, por favor, para los actores.

No se vayan a sentar. Sigan de pie. Vamos a ver cómo DNSSEC resuelve este problema. Por eso están aquí. DNSSEC fue inventado mucho más recientemente que el resto de la DNS. Son las extensiones de seguridad las que manejan este tipo de problemas. Lo que les voy a mostrar ahora es la importancia del DNSSEC. Cada registro que es transferido está firmado de tal manera que está encriptado y nadie lo puede modificar. Desde la raíz hasta abajo. Ahora los actores les van a mostrar cómo funciona esto.

ORADOR SIN IDENTIFICAR: Muy bien. Ahora yo sé que existe el DNSSEC. Como usuario, hago la validación del DNSSEC para asegurarme de sólo recibir consultas autenticadas. Entonces escribo nuevamente. ¿Perdón? Ahora tenemos la raíz, .com, .big bank, todos con DNSSEC. Ahora tienen el color amarillo. Y este es el procedimiento que hace el gTLD para crear firmas digitales para todas las respuestas que van a dar.

Ahora estoy más confiado en hacer mi transacción financiera con el DNS. Quiero ir a www.bigbank.com.

ORADOR SIN IDENTIFICAR: ¿Cómo te gusta ir ahí, eh? Hola Raíz, un usuario quiere ir a www.bigbank.com. ¿Dónde está?

ORADOR SIN IDENTIFICAR: No estoy segura, pero sé dónde está .com, está en 1.1.1.1. Pero tengo que firmar esto primero.

ORADOR SIN IDENTIFICAR: Lo voy a chequear. Si es el mismo color sí que te creo. Hola .com, un usuario quiere ir a www.bigbank.com. ¿Me puede decir dónde está?

ORADOR SIN IDENTIFICAR: No sé dónde está www.bigbank.com, pero sé dónde está bigbank.com. Es 2.2.2.2, y tengo una firma también para que sepas que es real.

ORADOR SIN IDENTIFICAR: La voy a chequear. Está bien. Voy a ir con bigbank.com. Hola bigbank.com. Uno de mis usuarios quiere ir a www.bigbank.com.

ORADOR SIN IDENTIFICAR: Yo sí te puedo ayudar. Está en 6.6.6.6.

ORADOR SIN IDENTIFICAR: Pero no hay firma. ¿Dónde está? De verdad.

ORADOR SIN IDENTIFICAR: Yo sí te puedo ayudar. Está en 2.2.2.3, y aquí está mi firma.

ORADOR SIN IDENTIFICAR: Excelente. Hola usuario, 2.2.2.3, esto yo lo chequeé, tengo la firma y está todo bien.

ORADOR SIN IDENTIFICAR: Muy bien. Ahora estoy mucho más tranquilo. Puedo ir al banco y hacer la transacción. Gracias.

WES HARDAKER: Muchísimas gracias a los actores tan talentosos que tiene la ICANN.

Ahora vamos a seguir y en lo que queda de nuestra sesión, la próxima hora exactamente, vamos hablar con más detalle acerca de cómo funciona el sistema.

Algo que tienen que entender es que el DNSSEC protege al DNS. Si le hacemos una pregunta al sistema de nombres de dominio, recibimos una respuesta. Eso no significa que protegemos todo Internet. Se protege sólo al DNS. Hay otras tecnologías que protegen a los otros sistemas, como el sistema de enrutamiento con su propia tecnología. HTTPS es la tecnología TLS. Entonces lo que tratamos de proteger con DNS es cómo obtener la

respuesta correcta, no necesariamente el resto de la infraestructura de la experiencia de navegación.

La solución DNSSEC es la solución que da respuestas y que ha estado implementada desde hace más de una década y que cada vez más. No sé, hace cinco o diez años. No, diez o veinte años ya.

Muchos de los TLDs tienen estas firmas. Hay algunos que tienen distintos niveles de despliegue. Las claves y las firmas cumplen el propósito de verificar la información y las claves pueden solicitarse a todo lo que está por debajo de la raíz. Son las claves para hacer la verificación de todos los pasos en el DNS.

En definitiva, el DNS es un sistema de búsqueda, y simplemente se puede solicitar la clave necesaria. La que necesitan en la parte superior es la que está en la raíz.

El resolutor sabe cuál es la clave. Tiene que saber desde antes cuál es la clave preconfigurada. Cathy es la Raíz, es la que tiene que hacer lo mismo que todo lo que viene después, incluida la clave, en este caso de bigbank.com y de .com. Hay lo que se llama cadena de confianza de arriba hacia abajo.

Lo que ustedes vieron con los actores visualmente es lo que vemos en este diagrama. Los recuadros con la tilde son los verificados, con las respuestas verificadas a través de la clave. Si

alguien intenta dar una respuesta inválida es sencillo verificar esto criptográficamente.

Ya hicimos la parodia, entonces ahora vamos a ver un ejemplo de por qué se necesita DNSSEC y una guía sencilla de cómo instalarlo.

¿Por qué debemos preocuparnos por el DNS? Seguramente a ustedes no les resulta fácil memorizar una dirección IP de cada sitio que quieren visitar, cada banco… pues los números telefónicos son difíciles. ¿Cuántos números telefónicos mantenemos en la memoria? Muy pocos, porque tenemos una base de datos de números telefónicos. Pero los números son muy difíciles de recordar. De hecho yo ya ni siquiera recuerdo los números telefónicos de mis mejores amigos. Y bueno, el DNS cumple este propósito. Conecta la forma en que nosotros pensamos los números con la forma en que las computadoras piensan los números. Y las direcciones de Internet utilizan números.

Algo a recordar es que todas las aplicaciones requieren el DNS para que los humanos puedan interactuar con ellas. Y si el DNS no funciona bien, los usuarios no van a poder ir al lugar al que pretenden ir.

El problema de esta falsificación es que la gente puede ser redirigida al lugar incorrecto a través de una dirección

incorrecta. Y hay varias maneras de ser redirigido en Internet. El ITF intenta determinar las distintas capas desde lo que es DNS. Hay que empezar por dar la dirección correcta y esto incluye la capacidad de proteger de que gente mala como el Dr. Malvado que vimos en los actores nos dé la respuesta incorrecta. Si la respuesta es incorrecta entramos al sitio incorrecto, podemos estar dando el número de pasaporte a un sitio de equivocado, un sitio malicioso que tiene actividad maliciosa o *malware*. De hecho es muy sencillo encontrar herramientas en Internet que concreten ataques a intermediarios, como se llaman en la comunidad de la ICANN. En la comunidad técnica tratamos de desarrollar esta tecnología para que este problema desaparezca por completo.

Entonces, ¿de qué manera nos sirve DNSSEC? Como explicaba, DNSSEC nos asegura llegar al lugar correcto. Lo más importante es tener la dirección correcta para llegar al lugar correcto. Y el secuestro será prevenido por las firmas, que eran representadas con las etiquetas de color en las tarjetas de nuestros actores.

Les pido disculpas, aquí tenemos un mal funcionamiento técnico.

Pensemos entonces en el mismo escenario en el que estamos desde el punto de vista de una representación gráfica. Lo vamos a ver varias veces porque queremos que entiendan claramente

qué es lo que pasa. Es muy difícil, es una secuencia compleja, y les vamos a mostrar cuán compleja es en un rato. Este es el diagrama de lo que acaba de pasar. Cuando llega una solicitud inicial atraviesa muchos servidores diferentes. Y acá podemos ver la cantidad mínima de flechas que tenemos. Vemos que hay muchas transacciones y hay mucha gente que no se da cuenta al teclear www.bigbank.com que de hecho se desarrollan muchísimas transacciones. Mucha gente piensa que es un solo pedido al DNS pero potencialmente podrían verse involucrados muchos servidores. Y vamos a ver después una diapositiva que muestra cuántos servidores de DNS se involucran en el acceso a una sola página que también tiene JavaScript y otro tipo de cosas involucradas.

En última instancia lo que queremos es la respuesta correcta para llegar al usuario Joe, que está abajo del todo a la izquierda. Tenemos un sitio web que se llama DNSSEC-deployment.org. En esta página web encuentran todo tipo de información acerca de cómo empezar a implementar DNSSEC, tanto dentro de su propia estructura para validar consultas como para hacer cómo firmar su propia zona raíz, si ustedes son dueños de una zona raíz. Hay algunos registradores que lo hacen. Hay herramientas disponibles en este sitio web por si ustedes lo quieren hacer por su cuenta.

Y luego hay herramientas para implementar un resolutor que sepa cómo hablar con DNSSEC y cómo hacer la validación. Fíjense que acá hay un tilde verde, en el margen superior izquierdo. Si uno de ustedes entra en este sitio web y ve ese tilde, eso indica que se está haciendo validación del DNSSEC. Si ustedes ven este diamante, este triángulo amarillo, esto significa que no está protegido el DNSSEC.

DNSSEC puede implementarse en diversos lugares. En general se lo hace el resolutor de ISP. Y de eso depende que les den buenas respuestas o no. También pueden hacerlo en el laptop, es un poco más difícil, yo lo hago pero yo soy un técnico. En general los dueños de los resulotores, los ISPs, son los que implementan el ISP local porque así protegen a todos los que están dentro del ISP.

Este el mismo diagrama que vimos antes. No voy a ir mostrando a dónde van todas las flechas, pero en última instancia vamos a ver acá que el Dr. Maldad, que está abajo, da una respuesta más rápidamente que todos los demás. El Dr. Maldad está muy cerca de la fuente que hizo la pregunta. Lo único que tiene que hacer es saltearse el resto de la estructura. Si el Dr. Maldad puede llegar más rápidamente que el resto va a ganar porque el DNSSEC se cree lo primero que llega, independientemente que provenga de una buena o mala persona o un mal servidor. En este caso llegó la flecha roja más despacio que el hacker del Dr.

Maldad, por eso el usuario creyó a quien le dio la primera respuesta. Esta versión es la misma pero ahora vemos que la mala respuesta del Dr. Maldad está bloqueada porque si bien llegó primera, fue chequeada por DNSSEC, fue chequeada por las firmas criptográficas que demostraron que esta respuesta no es la correcta y simplemente la tira y dice "Esta no la voy a aceptar, voy a seguir escuchando, vamos a ver qué más surge." Esto es exactamente lo que pasó antes en la parodia, cuando finalmente la respuesta final llegó al usuario.

Esto es lo que está ocurriendo con ese tilde verde. La primera respuesta vuelve pero llega más rápidamente, y si tienen un navegador que sabe hacer esto o si lo hace el ISP local, esa mala respuesta va a ser ignorada.

Este es un *spoofing* que hicimos nosotros en la última empresa para la que trabajé, donde insertamos un artículo falso en la página web utilizada solamente para *spoofing* del DNS, falsificación del DNS. Fíjense que la primera no tiene la página de Steve Crocker, sí la segunda porque notros lo incluimos.

¿Recuerdan que dije antes que el navegador web produce muchísimas preguntas? Este diagrama lo creé hace unos diez años ya, para serles franco, y cada una de esas líneas es una pregunta o una respuesta del DNS que surge simplemente cargar la página. Es así de loco. Y las cosas han empeorado

porque esto lo hice hace diez años y todo es peor aún hoy. Nosotros tenemos que asegurarnos de que cada una de estas líneas esté protegida para asegurarnos de que el navegador vaya al lugar correcto.

DNSSEC es un sistema muy complejo. Y los usuarios no tienen idea de cuántas consultas de DNS se hacen todos los días para hacer cosas simples como mirar un correo electrónico, mirar páginas webs, comunicarse a través de aplicaciones de mensajería, etc. hay mucha actividad de DNS y esta es una versión diferente del mismo diagrama.

Vamos a ver algunos aspectos básicos sobre DNS. Brinda la traducción de nombres a direcciones de red. Pero como vimos antes, DNS también puede cuestionar otras cosas. Podemos preguntar las claves, los nombres inversos, vamos a decir “si tengo el número, quiero el nombre”. Podemos preguntar, “¿cuál es el servidor?”. Hay muchas otras cosas. Es un sistema de búsqueda por clave.

Y el punto importante es que lo que cuenta son los datos. Cuando hacemos la pregunta, tenemos que asegurarnos de recibir la respuesta correcta. No nos importa cuántas personas ya lo manejaron antes. Y es una de las cosas fantásticas sobre DNSSEC, proteger los datos.

Entonces, si yo le doy la respuesta a la primera persona que está acá y hace todo el recorrido por esta sala, hace toda esta secuencia. ¿Se acuerdan del teléfono descompuesto al que jugamos de niños? ¿Cuando uno va susurrando una respuesta y la respuesta que llega al final es totalmente diferente? Esto no afecta a DNSSEC porque independientemente de cuantas personas lo toquen, aun si lleva un año recorrer toda esta sala, yo igual voy a poder verificar que esa respuesta no se haya modificado desde que se creó inicialmente.

Este diagrama también lo creé yo hace mucho tiempo. Y muestra todos los pasos diferentes que tienen lugar cuando creamos y publicamos datos de DNS. La persona que está a la izquierda dice, “Necesito crear un registro www. ¿Cómo lo hago”

Bueno, se lo agrega al dato de la zona, se lo publica en el servidor autorizado, el que es responsable de devolver respuestas. El servidor recursivo envía la solicitud al servidor autorizado para recibir la respuesta y el cliente a la derecha también envía la solicitud al servidor recursivo. Y fíjense que así comienza la cadena. El cliente envía una solicitud, la solicitud luego va al servidor autorizado, vuelve la respuesta y luego vuelve a este casillero. Y esta es una sola acción en comparación con las miles de líneas que vimos antes. Esta es una sola respuesta.

DNSSEC – voy a saltear algunas diapositivas porque al final vamos a hacer algunas otras cosas que normalmente no solemos hacer. Es un beneficio agregado para ustedes hoy. Así que voy a saltear algunas para poder llegar a los hechos importantes.

Un concepto importante es que tenemos que proteger los datos de la zona así como protegemos DNSSEC. Si DNSSEC protege a los datos, ¿qué pasa si ponemos datos malos? DNSSEC les va a decir que los datos malos son correctos. Los datos malos no se alteraron desde uno que se equivocó, cometió un error al teclear y puso esos datos. Entonces la gente se concentra en las claves privadas, mantenerlas a salvo, pero se olvidan de proteger y de evitar que la gente ponga datos incorrectos. Tienen que recordar que no solamente tenemos que proteger la seguridad en relación con DNSSEC sino que también hay que proteger los datos de la zona de la misma manera.

Este es el mismo diagrama que vimos antes, pero muestra solamente las partes que agregó DNSSEC. Esas líneas que les voy a mostrar son las partes nuevas. Antes agregamos el registro a los datos de la zona y ahora vamos a firmar eso para llegar a los datos firmados, el servidor autorizado va a publicar los datos firmados en contraposición a los datos de zona originales. Y además el hecho de que estamos validando el resolutor discursivo implica que estamos en contacto con la clave. Saber

cuáles son las claves de la raíz y poder hacer un seguimiento hasta el principio implica que tenemos las firmas y los datos firmados que puede verificar el resolutor.

Esta es otra diapositiva que hoy vamos a saltear.

Julie; bueno, supongo que hay preguntas. ¿Hacemos preguntas antes de continuar?

JULIE HEDLUND: Después viene Rick.

WARREN KUMARI: ¿Rick? Bueno, mientras – ahí está, ahí está Rick. Corre, corre Rick. No, tranquilo, tenemos tiempo. Donde quieras.

RICHARD LAMB: Hola. Yo trabajo en la ICANN. Yo fui una de las personas al principio a las que le dijeron, "Vamos a hacer esta cosa de la firma de la zona raíz". Nunca antes habíamos hecho esto. ¿Y cómo hacemos que la gente confíe en nosotros?

A veces es difícil si uno está en la ICANN. No los escucho reír así que me parece que no entendieron el chiste. Bueno, como escucharon en esta muy buena presentación, en esta parodia que hicieron tan divertida, hay un factor clave que es importante acá. ¿Cómo hacemos que la gente confíe en esta clave? En

primer lugar nosotros realmente confiamos, desarrollamos un sistema con 21 personas de todo el mundo, 18 de las cuales no son de Estados Unidos, lo cual es muy importante, y todos tienen claves físicas.

Se reúnen cuatro veces al año para algo que se llama la Ceremonia de la Clave. Suena bastante extraño, críptico. Pero no lo es. De hecho, es un proceso común usado para autoridad de certificación. ¿Ven que hay un candado cuando entran a un sitio web seguro? Bueno, nosotros lo copiamos de ellos.

No vamos a reinventar la rueda. Todos estos documentos que están ahí los aprovechamos. Esto se hizo en 2010. Fue un esfuerzo de la comunidad claramente y la ICANN participó igual que VeriSign, y lo hicimos por el bien de la comunidad.

Entonces, ¿de qué se trata esta presentación? Ya pasaron seis años. Vamos a cambiar y vamos a crear otra clave. Algo que nos entusiasma mucho a algunos de nosotros. Pero el problema es que si cambiamos esta clave, tal y como se explicó antes, la clave está integrada a los resolutores y a gran parte de la red, entonces si cambiamos sin contárselo, todo va a dejar de funcionar. Y ahí la gente nos va a mirar muy mal. Vamos a quedar muy mal.

Parte de la razón por la cual doy esta presentación, parte de la razón por la cual me dieron tiempo acá, fue para concientizar a la gente, para avisarles de que va a pasar esto.

Como dije antes, quizá haya algunos términos raros como la Ceremonia de la Clave. Nosotros en la ICANN dedicamos cientos de miles de dólares para aprender algunos de los secretos de estos procesos utilizados por los autoridades de certificación y otros. Pero como estamos en la ICANN todo es abierto, nosotros les contamos todo, publicamos todos los documentos, ustedes pueden copiar esta información y usarla, e incluso les decimos dónde está la información.

Esto está cerca del Aeropuerto de Los Ángeles y este es un lugar a 23 millas de la base nuclear en Washington D.C., de la zona en Washington D.C., es un centro de datos. Ellos tienen su base de datos ahí y nosotros ponemos nuestra base de datos también.

Para que vean que esto es algo de la comunidad, el nombre Kaminsky fue elegido por un motivo en particular. Hay un dicho, él no es un enemigo [inaudible].

Puedo gritar simplemente, si quieren. Alejo el micrófono un poco. Muy bien.

Acá ven a Vint Cerf, el padre de Internet, que también participó en esto. Anne-Marie de Suecia. Hay personas de todo el mundo.

Esto es para que vean que esto es algo en lo que participan distintas personas. Y de hecho yo entiendo que en el corto plazo, quizás en los próximos meses, busquemos más personas además de esas 21 personas del resto del mundo.

Ya me dijeron esto un par de veces. Pueden ver que principalmente hay hombres. Me critican por eso. Sería bueno que hubiera más mujeres participando en este proceso. Y los requerimientos son que la persona tenga una actividad en la que comunidad del DNS y que haya diversidad geográfica. No buscamos políticos, no buscamos personas que estén tratando de hacer otras cosas.

Lamento perder tiempo, pero esto es algo nuevo y quería contárselo.

¿Por qué estamos cambiando la clave? Lo hicimos en 2010 y funcionó bien. Precisamos una buena higiene criptográfica. Probablemente nuestra clave sirva para más tiempo. Posiblemente pasen 30 años más hasta que alguien pueda descifrar esta clave.

Pero nunca se sabe. Los algoritmos cambian, se hacen descubrimientos con respecto a las claves, así que es bueno tener una buena higiene criptográfica. Pero el principal motivo es el segundo. Si no lo hacemos, no vamos a saber cómo hacerlo en caso de que tengamos que hacerlo sí o sí.

El último punto; dijimos que lo íbamos a hacer. Todos ustedes saben ahora que en estas reuniones de la ICANN, la ICANN no tiene autoridad legal sobre nada en cuanto a la raíz. Es un concurso de popularidad. La gente confía en nosotros porque hacemos lo que decimos. Cumplimos. Entonces nosotros prometimos que íbamos a cambiar esta clave en cinco años y eso es lo que estamos haciendo.

¿Quién se va a ver perjudicado? Bueno, por el momento a todos los que estamos acá nos encantaría que se implementara DNSSEC para todo. Pero no es así. Cerca del 15% de los usuarios de todo el mundo están detrás de un resolutor que hace validación de DNSSEC, que realmente hace DNSSEC.

¿Cuántos de ustedes alguna vez vieron 8.8.8.8? Eso es Google. Tres personas en Manhattan decidieron usar DNSSEC. Increíble. Realmente me impresiona muchísimo que sea este porcentaje de gente que lo usa, y estoy muy agradecido con Google por hacerlo. Entonces si nosotros hacemos las cosas mal, esto se podría ver afectado. Por supuesto, estamos en contacto con la gente de Google para asegurarnos de que ellos vean la nueva clave y de que la instalen.

Si configuramos mal esto, hay muchas cosas que van a salir mal. Si DNS no responde con la respuesta correcta o si no da una respuesta, todo se va a caer y todos van a empezar a llamar. No

nos van a llamar a nosotros. Porque la gente que va a pensar que Internet se cayó, que no funciona. Entonces es muy importante hacer esto cuidadosamente, lentamente, y por eso nos tomamos tanto tiempo para hacerlo.

Ya casi termino. Estos son los documentos, por si quieren mirarlos. Este es nuestro plan. Si les interesa, por favor, léanlo. Por supuesto, tenemos planes de emergencia en caso de que algo salga mal. Pero no creo que nada vaya a salir mal, de hecho creo que va a salir bien.

El otro día, esto fue el 27 de octubre, generamos la nueva clave. Todavía no está en Internet. Como dije, este es un proceso muy lento, vamos a dar pasos muy pequeños para llegar al final. Pero generamos la clave.

Esta es la foto por la que me criticaron, porque hay sólo hombres. Esto es malo. Entonces, ¿qué hacemos? Al igual que la primera vez, cuando se genera la clave, hay una página en donde se representa la parte pública de esta clave, todos la firmamos.

Habrá una segunda parte de esto en Los Ángeles, cerca del 2 de febrero. Entonces si van a estar en Los Ángeles en ese momento, por favor, pregunten y podemos incorporarlos. Esta Ceremonia de la Clave está abierta a todo el mundo. Todos pueden asistir y observar el proceso. Será aburrido, pero a veces tenemos una

buena cena después de la ceremonia. Bueno, como en ICANN. Ayer fue una buena fiesta. ¿No es cierto?

Bueno, estas son las siguientes fechas. Acá es donde se empiezan a ver las cosas en Internet, en el DNS. El 19 de septiembre van a ver que se introducen nuevas claves.

Pero el 11 de octubre de 2017 es la fecha clave. Ríanse. No, no se ríen. Es la fecha principal. Es cuando va a entrar la nueva clave. Parecería que faltara mucho tiempo, pero necesitamos empezar ahora a avisar para que después todo el mundo sepa que esto va a pasar. Creo que para los grandes va a estar todo bien, pero siempre puede haber alguien que no actualice la clave. Tenemos que avisar con anticipación. Algunos procesos optimizados. Acá, en esta diapositiva, que es mi preferida, tenemos todos los detalles de todo lo que se va hacer. Muy importante. Lo puse sólo como referencia.

¿Qué tienen que hacer entonces? Supongamos que 8.8.8.8, que es Google, quieren la nueva clave, la quieren configurar, y son gente inteligente y por ello saben cómo hacerlo. Todo bien. Y muchos de los grandes ISPs seguramente van a seguir el mismo patrón.

Pero también hay un proceso automatizado. Hay estándares. El IETF tiene normas. Vamos a seguir esta norma para actualizar

automáticamente la clave. Hay otras normas o abordajes automatizados que también van a permitir el traspaso.

Esto lo escribió un colega alemán que también trabaja en la ICANN, y él puso esto. ¿Qué pasa si algo no funciona bien? Esto es la gestión desde el ángulo negativo.

Creo que esto es todo. Tenemos algunos bancos de ensayo para desarrolladores, para la zona raíz.

Estos son materiales para gente que son resolutores, operadores o hackers. Gente que quiere testear los sistemas. ICANN también va a tener un banco de prueba que se dará en tiempo real. Son bancos de pruebas acelerados. Se mueven mucho más rápido que lo que pasará en tiempo real. Son cosas más complicadas. De todas formas si tienen preguntas más concretas me pueden enviar un correo electrónico a richard.lamb@icann.org.

Y también hablamos con los proveedores, con Microsoft, por ejemplo; y con muchos de los proveedores grandes, así que se pondrá en marcha. Bueno, eso es todo. Esto es lo de Twitter. Yo no uso mucho Facebook o Twitter, pero aquí está. Aquí es como me pueden contactar. La mejor manera es por correo electrónico, y si no les respondo de inmediato, bueno, me pueden castigar. Me pueden enviar otro mensaje y les voy a contestar.

Bueno, esta es mi presentación del traspaso de la clave. No sé si tienen preguntas. ¿Alguna pregunta en línea?

JULIE HEDLUND: Es una pregunta que entró. A ver cómo damos la prioridad. Esta es una pregunta remota de [Afifa Abbas] de Daca, Bangladés. La pregunta es, "¿Puede explicar el uso de la clave para la firma de la zona y la clave para la firma de la llave en DNSSEC?"

WES HARDAKER: Quiero agradecerle su presentación, Richard, puede tomar asiento. Excelente presentación.

Es una presentación adicional que normalmente no la tenemos en nuestro plan, pero por lo crítico de los futuros acontecimientos la hemos incluido.

En realidad es una pregunta que se puede hacer a cualquiera de los panelistas. Además, a los presentes si tienen preguntas sobre cualquier tema de DNSSEC o lo que presentó Richard, mientras llega el micrófono vamos respondiendo.

WARREN KUMARI: Hay dos cosas, que es la Clave para la Firma de Zona, la Clave de la Raíz es la clave para firma de la llave, cuyo propósito es firmar otras claves.

¿Por qué hay dos claves diferentes? Porque la de la firma de la llave no se usa con frecuencia, sólo se usa la de la firma de zona. Esto hace que el sistema sea más seguro. Se puede guardar la otra en una bóveda y mantener la seguridad.

Son dos niveles de seguridad. La Clave para la Firma de la Llave se puede guardar en una bóveda y se usa solamente la clave para la firma de la Zona.

No tengo idea si me entendieron.

WES HARDAKER: Una pregunta. ¿Podrías darnos un ejemplo, una Zona que necesita agregarse información con tanta frecuencia que la clave para la firma de la Zona también tenga que guardarse bajo llave?

WARREN KUMARI: Puedo nombrarte varias. Una es .com. A medida que se añade información a .com, que sucede minuto a minuto, se necesita estar firmando constantemente la zona .com con la clave para la Firma de Zona.

Además, con ciertos elementos criptográficos, cuanto más use la clave más fácil será para un atacante identificar esa clave. Por ello es una buena práctica cambiar esta clave con frecuencia. En

especial si se usa mucho. Esto significa que la de firma de Zona hay que cambiarla con frecuencia, es un proceso molesto pero si se tiene una clave Para la Firma de la Llave, perdón, hasta yo me estoy confundiendo. No es necesario preocuparse tanto por la parte molesta que representa cambiar las claves.

WES HARDAKER: ¿Alguna otra pregunta?

ORADOR SIN IDENTIFICAR: Otra razón operativa para tener dos claves es que si cambia la KSK, la Clave para la Firma de la Llave, hay como una entrega formal. Hay que decirle al nivel superior para que bigbank.com cambie su clave tengo que decirle a .com que hay otro clave. Entonces es más trabajo cambiar esta clave.

WES HARDAKER: Importante esa respuesta. Tenemos otra pregunta.

[AWAL}: Soy [Awal]. NextGen. Creo que gran parte del trabajo en el despliegue del DNSSEC es técnico e involucra en su mayoría a los ISPs y a los operadores de DNS. Como usuario, si yo veo que mi pedido no usa el DNSSEC, como usuario, ¿qué puedo hacer?

WARREN KUMARI: Lo que sí puede hacer, que es bastante molesto a menos que uno sea un fanático de las computadoras, es tener un resolutor validado en la propia máquina, y eso es mucho trabajo y es bastante dificultoso.

Otra opción es cambiar el resolutor del DNS a uno que haga validación de DNSSEC. Entonces, si el ISP en este momento no hace validación de DNSSEC puede habilitarse esta validación por DNSSEC, y si no hay resolutores como el de Google, que hace validación, cambiar el resolutor en la máquina. O sea, reconfigurar la máquina para que apunte a este resolutor.

Y también hay uno, creo que es el 64.64.6, no recuerdo el número, que es Open DNS. Hay varios resolutores abiertos que se pueden usar.

WES HARDAKER: En relación con esto, no hay un ser humano que pueda recordar esta cadena de números. Por eso tenemos DNS precisamente.

Antes de usted había otra pregunta por aquí atrás.

ORADOR SIN IDENTIFICAR: Soy de Egipto, becario por segunda vez, tengo un comentario y una pregunta. Como comentario, yo uso DNS, y mi pregunta es si la KSK es segura. ¿Es necesario o sirve hacer *rollover* de la

KSK? Y la pregunta, sobre el traspaso de la KSK, ¿hay que hacer una actualización de la confiabilidad del sitio?

DNSSEC no me asegura el vínculo con el ISP y no confío un resolutor local en mi máquina. ¿Qué consejo me pueden dar?

WES HARDAKER: Gracias por su pregunta. Esto es lo que nosotros llamamos el problema de la última milla, cómo tener una respuesta segura hasta el iPad o la computadora.

WARREN KUMARI: Una posible respuesta la dará mi colega. Con respecto al problema de la última milla, si a usted le preocupa que nadie manipule indebidamente la respuesta del ISP, hay dos opciones. Una es simplemente hacer un resolutor validado desde la laptop propia. Hay una herramienta que creo que se llama DNS Trigger, que es la más fácil, y es una aplicación que puede instalarse. Este resolutor se va a ocupar de hacer la validación concreta en el dispositivo para que los datos tengan seguridad de DNSSEC.

En algún momento el IETF está trabajando en otra solución que encripta la información de la laptop hacia el ISP. Es un grupo de trabajo que se llama Deprive y estamos tratando de privar a los atacantes de la capacidad de hacer cambios.

También su motivación es otorgar privacidad a las consultas. Si hay un atacante que sigue o ve las consultas sabe a dónde van. La idea es encriptar el DNS para que los atacantes tampoco lo vean y así se puedan bloquear.

WES HARDAKER: Una aclaración. Para encriptar la pregunta sólo le llega al resolutor, los datos no son almacenados en el DNS en realidad.

NAVEEN TANDOM: Hola, Naveen de India. Becario de ICANN. Un par de preguntas. ¿Por qué eligieron este sistema para la Ceremonia de traspaso la Llave?

RICHARD LAMB: No me acuerdo por qué hicimos este sistema así. Dos razones. Originariamente hay dos claves, ZSK, KSK. ZSK es más corta. Cuanto más corta es la clave, más fácil de comprometer.

Entonces se tiene que cambiar con más frecuencia la ZSK. Ahora se cambia cuatro veces al año. Cada Ceremonia de Clave es una nueva ZSK. Por eso se hace así. Depende a quien se pregunte, la respuesta de cuán seguro es será distinta. Cinco personas tendrán cinco respuestas diferentes. Seis meses irá una personas, dos meses irá otra. Si seis meses es un límite

razonable, la idea es bajar un poquito el umbral. Esa es la razón uno. La razón dos es más política. Esta gestión de la clave se hace entre ICANN y VeriSign, dos organizaciones. La idea es que la KSK firma la ZSK. Se coordina de a diez años por vez. ¿Porque qué pasa si no funciona? ¿Qué pasa si no nos llevamos bien con Verisign?

O sea, se pensó mucho. Pero el motivo principal por el cual se hace cada tres meses es una razón criptográfica.

NAVEEN TANDOM: Otra pregunta. ¿Sigue el 140 nivel 2-3?

RICHARD LAMB: Lo respondo rápidamente. ¿La pregunta es si seguimos confiando? Bueno, no tenemos otra opción. Se lo dejo a Warren. Pero básicamente seguimos una norma, la idea es que somos burócratas y tenemos que seguir una norma de seguridad. Hay una cosa que se llama ISO, la norma ISO, y cuando la ISO cambie sus normas nosotros vamos a cambiar lo nuestro también.

WES HARDAKER: Warren.

WARREN KUMARI: Sí, estaba respondiendo a lo que dijo Rick, qué opción tenemos. Bueno, en este momento hay un número bastante reducido de personas que hacen HSMs, pero que aseguran las claves criptográficas.

Hay muchas personas que han intentado atacar a los HSMs y en general son muy buenos. No obstante, muchos de los proveedores de HSM están basados o han estado basados en los Estados Unidos y hay posiblemente razones para no confiar en ellos.

Hay un proyecto en curso, que se llama Cryptic, que es un proyecto global que intenta atraer la mayor cantidad de países y que es de código abierto, de diseño abierto. Es un HSM proceso muy abierto para que cualquiera pueda validar el diseño y eventualmente construir el propio HSM y si tiene dudas de que el que tienen ha sido manipulado, pero es un proyecto muy grande, lleva muchos años. Los HSM son equipos costosos y complejos. Los HSM que usa ICANN, por lo que sabemos, son de los mejores que existen y parecen ser seguros.

WES HARDAKER: Gracias por su pregunta. Tenemos otra del piso.

ORADOR SIN IDENTIFICAR: ¿Los resolutores están abiertos a todo el mundo? Esa es mi pregunta.

WES HARDAKER: ¿Está preguntando que si todos los resolutores están abiertos a todo el mundo?

ORADOR SIN IDENTIFICAR: Sí.

WES HARDAKER: Buena pregunta. Warren, probablemente tú lo puedas responder.

WARREN KUMARI: Depende de qué resolutor estemos hablando. Tanto los autorizados como los de los servidores raíz están abiertos a todos los .com. Los que están en *server*, los que tienen la información y la ponen a disposición, esos en general son abiertos a todos.

La mayoría de los resolutores de los ISPs, por otra parte, sólo están disponibles a sus clientes, y eso se debe principalmente a razones de seguridad. Si se pusieran a disposición de cualquiera podrían tener ataques de consultas masivas.

También hay varias organizaciones que tienen resolutores recursivos abiertos. O sea, son los mismos resolutores que tienen los ISPs que buscan la respuesta en nombre de uno. Y hay varios abiertos. Por ejemplo el Google Public, VeriSign, Open DNS, que es un resolutor recursivo abierto muy conocido, y ellos ponen los resolutores a disposición mundial y la gente los sigue para mitigar los ataques de OT. 1:08

WES HARDAKER: Un agregado es por el hecho de que el resolutor sea abierto. Él mencionó que hay tres resolutores que tienen direcciones conocidas, 8.8.8.4 es uno, el de Google. Eso no significa que la infraestructura local sea ISP; el gobierno, lo que fuere, no les va a permitir acceder ahí.

Hay *firewalls* que previenen los ataques a intereses corporativos, que bloquean.

Entonces no hablamos de la política, aun así podemos no acceder a los resolutores abiertos si se envía una consulta y hay una política interna que la bloquea.

Otra pregunta.

ORADOR SIN IDENTIFICAR: Soy [Ian Harsh]. Y la pregunta que quiero hacer es, si tenemos un TLD de múltiples niveles, ¿opera en ese caso el DNSSEC? ¿Cómo se maneja la clave de zona en ese caso?

ORADOR SIN IDENTIFICAR: Usted dice, si tenemos dos niveles de zonas en el TLD…

ORADOR SIN IDENTIFICAR: [co].in es un dominio; [co].in en ese caso, ¿cómo opera el DNSSEC? Porque hay tres niveles por lo que ustedes mostraron.

ORADOR SIN IDENTIFICAR: Hay dos formas. Se firma .in y luego se firma [co].in y se genera una cadena de confianza entre ambos y con [co] se firma otra zona, esa es una forma.

Y la otra forma de hacerlo, [co] y luego se trata como una terminal de no entidad, entonces se firma todo en el tercer nivel dentro de la zona junto con la misma clave para .eu, por ejemplo, como tenemos nosotros. Podemos usar co.eu para firmar el propio.

WES HARDAKER: Lo voy a contestar distinto. Una de las cosas que dejamos fuera de la parodia, porque se tornaría muy complejo, es que en cada una de las claves hasta abajo podemos tener hasta 25 niveles, y

en tanto en cuanto se empiece desde la raíz hay un vínculo seguro entre cada padre y cada hijo, es decir, la raíz conoce el vínculo para .in y sabe de dónde sale la clave, y este es el vínculo seguro, entonces .in va a decir "un momento, yo a mi vez tengo subordinados, si hoy es uno, este el vínculo seguro". Entonces el resolutor que hace todo este encadenamiento llega hasta a.b.c.e., hasta llegar al vínculo seguro correcto. Y así se verifica la respuesta. O sea, todos en la cadena son verificados.

Tenemos una pregunta desde aquí adelante.

[SARATA]: Soy [Sarata], de Ghana, becaria. Creo que mi respuesta ya fue respondida con esta última respuesta. Pero de todas formas, esa persona maliciosa entró al sistema. ¿Esa persona puede conseguir la firma y regresar? ¿Hay alguna manera de evitar que vuelva a acceder si consigue la firma?

WARREN KUMARI: Una de las cosas que hacemos es la siguiente. Tratamos de simplificar las cosas. Pero la mala persona, el Dr. Maldad, digamos que se fue, porque es malo.

A veces, en una de las parodias que hacemos, viene la firma. ¿Cómo detectamos que esto es un problema? .com se comunica con bigbank.com. Big Bank le dice a .com cuál es la firma. Y así

cuando el resolutor, el ISP le pregunta a .com, "¿Dónde está www.bigbank.com?", le dice "Big Bank está ahí y su firma es como esta".

Entonces cuando el ISP va a bigbank.com, sabe cómo debería ser la firma. Cuando el Dr. Maldad viene y trata de dar la respuesta incorrecta, el ISP ya sabe cómo debería ser la firma de bigbank.com y la puede comparar y ver que no coincide.

No sé si respondí claramente a su pregunta.

WES HARDAKER: Un mensaje importante es que, como dije al principio, DNSSEC protege el DNS, no nos protege contra otras clases de ataque que se producen fuera del DNS, una de las cuales es la ingeniería social. Si alguien llama a .com y le dice, "Yo soy bigbank.com, necesito cambiar mi clave", eso podría ocurrir como ataque de ingeniería social.

DNSSEC no nos protege de eso. Esa es función del registrador dentro del mundo de DNS, asegurarse de que hagan la verificación de quién es usted cuando llama para decir, "Tengo que cambiar los datos".

Esas clases de ataque también tienen que encararse, pero la forma es totalmente diferente de lo que hace DNSSEC. En DNSSEC también se avanzó mucho para cubrir algunos temas

que están un poquito fuera del alcance del debate de hoy sobre el DNSSEC.

ORADOR SIN IDENTIFICAR: Tengo dos preguntas. ¿Voy una por una o digo las dos?

WES HARDAKER: Diga las dos.

ORADOR SIN IDENTIFICAR: Toda esta idea de DNSSEC es fantástica, pero también sé que sigue habiendo unos ISPs que no implementan DNSSEC. ¿Cuál es la razón?

WES HARDAKER: Muy buena pregunta.

ORADOR SIN IDENTIFICAR: La segunda pregunta es que sabemos también que hay algunos proveedores de servidores recursivos que no pasan por la raíz porque llegan a la zona raíz a través de la IANA. Warren, creo que usted sabe de qué hablo. ¿Esto no puede afectar este canal de confianza?

WES HARADAKER: En términos de – estoy tratando de recordar su primera pregunta. Ah, por qué la gente no lo implementa.

Bueno, hay un par de razones. Por un lado, no he escuchado hablar de esto. Por eso tenemos estas sesiones. Porque todavía estamos en la fase educativa del mundo. No todo el mundo sabe esto.

En segundo lugar, hay muchos ISPs que tienen menos personal del necesario y quizá quieran hacerlo pero simplemente no tuvieron el tiempo para incorporar las cosas nuevas. La buena noticia es que el software de los resolutores por *default* lo van a activar cuando implementen la próxima versión, quizás automáticamente lo pongan, lo incluyan, aun quizás sin saberlo porque de manera predeterminada lo van a incluir.

Además, muchas veces los usuarios no lo piden. Usted llama al ISP y le dice, “Acabo de ver que usted no me está protegiendo, ¿podría hacerlo por favor?”. Si reciben suficientes consultas de los clientes quizá tengan la motivación y quizá le den una respuesta y le expliquen por qué todavía no lo hicieron.

Hay que preguntarle a cada uno el por qué, de forma individual, estoy seguro. Yo ya escuché todas estas respuestas anteriormente, “No tengo el personal necesario”, “Nadie me pidió que lo hiciera”. Algunos dicen, “No lo conozco lo

suficiente", "No lo entiendo bien", "Tengo que obtener más información primero". Todas estas son razones que yo escuché.

Y quizá Warren quiera responder a la segunda pregunta.

WARREN KUMARI: La segunda pregunta es muy buena. Les voy a dar un poco de información general. Hay un documento del IETF que dice que los resolutores pueden simplemente conservar una copia de la zona raíz dentro de sí mismos para no tener que salir a preguntarle a la raíz.

Esto no altera DNSSEC porque cuando esos resolutores bajan la copia de la zona raíz, la zona raíz contiene todas estas firmas para todos los dominios de alto nivel que están dentro del mismo.

Entonces cuando funciona DNSSEC, en lugar de salir a preguntar a la raíz, busca dentro de sí mismo y tiene todas las firmas ya allí. O tiene todos los numerales para las firmas técnicamente. Pero puede hacer la verificación hasta el final. Simplemente no tiene que enviar una solicitud por separado a la raíz.

WES HARDAKER: La clave que está allí es propiedad de la IANA, que forma parte de la ICANN. Todos los servidores, independientemente de que

sean personales, los servidores raíz, si bien hoy en el tutorial de servidores lo sabrán.

Y ustedes pueden verificar que ellos no lo hayan modificado. Porque la cadena de DNSSEC comienza con esa clave, y si uno conoce esa clave y la clave de la que hablaba Rick, pueden verificar lo que todos dicen.

Y una vez más, aun si recorriéramos toda esta sala independientemente de dónde obtenemos los datos, DNSSEC no protege la transacción entre ustedes y yo, protege la transacción que dice que nadie desde que la ICANN la publicó la modificó. Y eso me incluye a mí, a ustedes y a todos los que la hayan tocado mientras tanto.

WARREN KUMARI: Y la razón por la cual existe este documento *loopback* es por la protección que mencionó Wes. El hecho de que DNSSEC firma todos los registros significa que se pueden tomar los datos de cualquier lugar, no importa, aun si encuentran los datos en un pedazo de papel en el piso. Si están validados no importa de dónde vienen. Así que podrían tenerlo dentro de sus propios resolutores.

WES HARDAKER: Muy buena pregunta. ¿Hay otra pregunta?

ORADOR SIN IDENTIFICAR: Tengo una pregunta breve relacionada con el desempeño. ¿Cuánto gasto adicional genera este proceso? Encriptamiento, trabajo con las claves…

WES HARDAKER: Es una muy buena pregunta. Cuánto sufrimiento implica hacer toda este higiene criptográfica. ¿Alguien tiene algunos datos recientes? ¿Rick? ¿[Jack]?

[JACK]: ISOC escribió un documento sobre este tema hace unos cinco años. Y en esa época genéricamente era un 10% más de carga sobre el DNS. Pero eso fue hace cinco años. Yo diría que hoy la diferencia es mínima, la diferencia en *performance*.

WARREN KUMARI: Lamentablemente, al igual que en cualquier pregunta técnica, depende y es complejo. Entonces cuando hablamos de carga y desempeño depende a quien le hagamos la pregunta se necesita más búsqueda de DNS, hay más tráfico por tanto se necesita más ancho de banda.

Pero creo que lo que él está preguntando es CPU o carga sobre el resolutor. Para hacer la validación, yo vi algunos números publicados que son menores al 1% de carga para la CPU.

Eso es un porcentaje mínimo. No es un porcentaje importante. Eso para la validación. Hay búsquedas adicionales pero se guardan en la memoria caché, por lo tanto también es mínimo.

La respuesta general es, no lo suficiente como para que la gente se dé cuenta.

WES HARDAKER: Gracias.

NASRAT KHALID: Hola. Yo soy Nasrat, de Afganistán, y mi pregunta es acerca del DNS público. ¿Por qué es gratuito? ¿Por qué Google está tratando de hacernos este favor?

Y la próxima pregunta es acerca de las complicaciones cuando utilizamos este DNS público, tenemos complicaciones en nuestras propias redes, yo he visto esto varias veces. Y la latencia o cuánto demora esto, la resolución del nombre de un *host* en comparación con un DNS localizado.

WARREN KUMARI: Yo podría responder ambas preguntas con la misma respuesta. La razón por la cual Google ofreció esto es porque la latencia baja es muy importante para los usuarios. Si las solicitudes de los usuarios llevan mucho tiempo se aburren y no usan tanto Internet. Muchos ISPs tienen resolutores muy lentos y por eso Google ofreció esto, porque Google quiere ganar dinero, Google ofreció esto porque significa que los usuarios tienen una experiencia en Internet más rápida, lo cual significa que usan más Internet y eso significa que ven más avisos, más publicidad y Google gana dinero con eso.

Entonces Google no cobra por el servicio pero hace que Internet sea más rápido y también garantiza que los usuarios reciban la información correcta.

Hace unos años había algunas empresas que brindaban respuestas falsas. Si uno escribía mal un nombre le enviaban información de otra persona, entonces Google se asegura de que los usuarios reciban las respuestas correctas, que hagan que los usuarios estén satisfechos y que usen más Internet.

La latencia del DNS publico debería ser mejor que el del ISP. Y si no, debería usar el resolutor del ISP. Si el DNS público de Google no le simplifica las cosas, entonces no lo use.

¿Respondí ambas partes de su pregunta?

WES HARDAKER: Creo que esa fue una muy buena respuesta. ¿Está de acuerdo?

NASRAT KHALID: [Inaudible]

WES HARDAKER: Está hablando acerca del lado de los datos.

NASRAT KHALID: [Inaudible]

WARREN KUMARI: La política de privacidad del DNS público de Google está en la web. Dice qué información registramos, registramos poca información para identificación de fallas, pero esa información pasa a ser anónima y se comprime. Todo eso se publica en línea en www.google.com/developers/public. No recuerdo, pero si *googlean* "Google DNS privacidad" van a encontrar la información, y yo diría que todo eso es cierto. Si no fuera así, las cosas van a terminar muy mal. Pero yo puedo decir que esto, que la información que ellos publican, es correcta y es cierta.

WES HARDAKER: Gracias.

[BETTINA]: Yo soy [Bettina], miembro del Programa de Becarios de Tailandia. Nosotros estamos tratando de impulsar el tema del DNSSEC en Tailandia. Una cosa que me resulta difícil es pelear por el presupuesto, porque es un tema muy complejo, la gente no lo entiende. Es un tema tan técnico, tan complejo que cuando digo esto me contestan, "Bueno, para los hackers también va a ser difícil y complejo". En comparación con otros ataques cibernéticos, ¿qué porcentaje de peligro hay? ¿Ustedes tienen datos o investigación?

WES HARDAKER: Es una muy buena pregunta y sirve para responder unas preguntas anteriores, porque la gente no implementa validadores hoy. Todo se remite a una cuestión de presupuesto. El tiempo de la gente implica un costo. Implementar cualquier cosa nueva implica un costo. Rick.

RICHARD LAMB: Dado que obviamente yo tengo la religión del DNSSEC, sólo voy a decir cosas buenas acerca de DNSSEC.

Para muchos de nosotros no se trata de proteger el DNS. Yo estoy muy entusiasmado. Piense en un sistema en el que podamos intercambiar material público clave de forma segura

entre todos. Digamos que yo quiero enviarle un mensaje encriptado de extremo a extremo. Ahora lo puedo hacer.

Uso el DNS, busco la clave, encripto el mensaje en mi laptop, eso va a su laptop, usted usa mi clave o la copia de mi clave, etc.

La idea es que se convierta en una base de datos protegida a nivel global que la gente pueda usar para intercambiar información. Eso es lo bueno, lo interesante. Vint Cerf ya dijo esto hace muchos años, en 2010 dijo, "Acá está pasando algo mucho más importante".

Esa es parte de la respuesta. La otra parte de la respuesta es que esta infraestructura con el 90% tiene implementado DNSSEC, la primera fase, no la segunda. Pero esa es una oportunidad para algunos de nosotros.

WES HARDAKER: Otra cosa que puede hacer es *googlear* "DNS hijack", secuestro del DNS, van a ver que hay muchos artículos acerca de casos que ocurrieron en la realidad. No tengo acá inmediatamente una referencia, no me recuerdo una referencia de memoria, pero hay toda una serie de casos, hay muchos artículos que se publicaron sobre cosas que se secuestraron, sitios web que se contaminaron, y eran sitios que no tenían DNSSEC.

Esto podría ser información que usted puede usar y que cualquiera puede utilizar para decirles a otros, “Estos son los casos que ya ocurrieron. Esto es muy común.”

¿Protege todo? No. Esto se remite a lo que dije al principio. Para proteger todo hay que chequear todas las capas de Internet y el IETF está trabajando mucho para proteger cada vez más capas.

ORADOR SIN IDENTIFICAR: DNSSEC es una plataforma para la innovación. El futuro de Internet, el Internet de las cosas conecta todo con todo, eso es IPv6. El Internet de las cosas obviamente necesita mucha seguridad, y eso es DNSSEC. Y eso es central para la infraestructura.

Así es como lo vendemos. Ustedes quieren el futuro, entonces van a tener que tener IPv6 y DNSSEC.

WES HARDAKER: ¿Hay alguien que todavía no haya hecho una pregunta?

[GIGI]: Gracias. Yo soy [Gigi], soy de Estados Unidos, y me preguntaba si podía explicarnos cómo se implementaría DNSSEC en un nuevo gTLD y cómo afectaría esto a los registratarios.

WES HARDAKER: ¿Alguien quiere hablar acerca del modelo de los nuevos gTLD? ¿Rick?

RICHARD LAMB: Yo puedo hablar, pero no trabajo mucho en el área de los nuevos gTLDs. Todos los nuevos gTLDs tienen que implementar DNSSEC. La mayoría de los proveedores de *backend*, cuando yo digo esto, muchos gTLDs tienen otras personas que están a cargo de su infraestructura. Y, en general, tienen muchos conocimientos DNSSEC. ¿Cómo lo implementan? Bueno, pueden asistir a uno de mis cursos. Yo doy un curso de cuatro a cinco días en distintas partes del mundo. Lamentablemente en Estados Unidos todavía nadie me lo pidió, así que usted quizá sería la primera. Muestra cómo implementar todo el sistema, con la Ceremonia de la Clave, con el *software*, con las claves, etc. Todo esto lo pueden hacer ustedes mismos.

Si no quieren hacerlo, si no quiere utilizar uno de los proveedores de *backend* que ya existen y que ofrecen esto, hay algunas soluciones comerciales disponibles. Puede elegir una u otra. Yo personalmente creo que debido a que DNS requiere ciertos conocimientos es mejor que implementen estas cosas ustedes mismos, al menos para entenderlo, para que cuando haya algún problema ustedes sepan cuál es el problema. No sé si esto responde a su pregunta.

WES HARDAKER: Muchas gracias. Ya casi nos quedamos sin tiempo, pero queda tiempo para una pregunta más antes de dar por cerrada la sesión.

[AWAL]: Soy participante del Programa NextGen. Si yo tratara de resolver un dominio, por ejemplo si viene el Dr. Maldad y trata de hacer algo, como usuario, si DNSSEC ya está funcionando, como usuario, ¿puedo recibir información o alguna notificación de que alguien haya tratado de quebrar esa cadena de confianza? Como usuario, ¿voy a recibir alguna notificación?

WES HARDAKER: ¿Rick? ¿Warren?

WARREN KUMARI: Como usuario probablemente no reciba nada. Es muy difícil para un usuario común identificar que alguien trató de hacerlo porque el resolutor que está arriba simplemente va a ignorar esa respuesta, no le va a decir que alguien trató de mentir.

Si usted tiene su propio resolutor, en ese caso puede buscar los archivos de registros, y en ellos se indicará que recibió un paquete malo, pero básicamente el usuario final nunca debería ver la respuesta mala del atacante. En términos generales ni se va a enterar porque como no llega esa respuesta equivocada no marcará ninguna diferencia.

No sé si esto responde a su pregunta.

WES HARDAKER: Esa ha sido una muy buena respuesta. Yo quiero agregar que hay una aplicación que realiza los archivos de registros y le indica si pasó algo así, pero esto hay que hacerlo de forma local en el laptop.

¿Cómo vamos con el tiempo? ¿Tenemos tiempo para una pregunta más?

JULIE HEDLUND: Una última pregunta.

WES HARDAKER: Una última pregunta antes de dar por cerrada esta sesión.

Por favor, use el micrófono.

ORADOR SIN IDENTIFICAR: Casi percibió mi pregunta porque él hizo la pregunta acerca del usuario final y usted dijo que hay que instalar el sistema localmente. Y mi pregunta es si esto se puede hacer con un navegador, quizá lo podemos instalar sea cual sea el navegador y de esta forma enterarnos.

WES HARDAKER: Muy buena pregunta, la voy a responder yo porque de hecho yo escribí un *plug-in* para el *browser* que hace esto. hay para Chrome y para Firefox. Está en el repositorio de *plug-ins* y atrapa la mayoría de las cosas porque no busca todas las búsquedas de DNS que hacen. Hay muchas cosas técnicas ahí por las cuales no es técnicamente perfecto.

En mi empresa escribimos el *plug-in* para Firefox. Nosotros escribimos uno y lo hacemos a nivel del usuario, pero así como su ISP le saca muchos otros problemas con, por ejemplo, el enrutamiento y cómo llegan los paquetes al lugar correcto, también les saca problemas en cuanto a búsquedas de DNS. En términos generales el usuario final no tiene por qué saber que el ISP lo protegió de algo malo. Los ISPs ya están haciendo eso. Ya hacen *firewalls*, hacen enrutamiento y ya hacen *lookup* de DNS, ya están gestionando los cables, ya gestionan las cajas y los casilleros.

Hay muchas cosas que hacen que ustedes no saben, así que yo diría que si entra un paquete malicioso, esa probablemente sea una de las cosas más de las que el usuario final no se enterará a menos que sea un especialista técnico como yo.

JULIE HEDLUND: Una pregunta más en el chat.

Hay una pregunta de Paul que dice, "¿Algún TLD implementó DANE ya?"

WES HARDAKER: Es una muy buena pregunta. Los TLDs en general no necesitan DANE. DANE es una tecnología de la que no hablamos acá. Tiene que ver con cómo asignar certificados de una autoridad certificadora o no al DNS y cómo las verifica a través de una cadena independiente.

Los TLDs, de hecho, no hacen eso. Porque los TLDs en general no tienen certificados. Pero los usuarios finales sí, y de hecho en las listas de *mailing* es donde más se aprovecha DANE. Si hacen una búsqueda de DANE y SMTP van a ver que hay muchos documentos de todos sitios web que cataloga, creo que en el último caso había 300000 dominios y muchos venían de ISPs de Alemania, que querían que esto ocurriera.

Rick, ¿quiere agregar algo?

WARREN KUMARI: Rick dijo que el DNSSEC protege al DNS y también crea una plataforma para poder hacer otras cosas. DANE es una de las cosas que permite hacer.

Y si Wes decía que ahora se está utilizando mucho en *mailing*, NES, que es el organismo de estándares de Estados Unidos, publicó algo donde sugiere utilizar esto, y hay una organización alemana de seguridad de la información o algo así que también sugirió enfáticamente que se utilice DANE en los correos electrónicos.

WES HARDAKER: Muchísimas gracias a los miembros del panel por habernos ayudado esta tarde.

Si tienen alguna pregunta, recuerden que el sitio web de implementación de DNSSEC existe desde hace mucho tiempo. Hay muchas respuestas para este tipo de preguntas.

Muchas gracias.

JULIE HEDLUND: Muchas gracias a Wes, el gran y único Wes. Gracias.

[FINAL DE LA TRANSCRIPCIÓN}