BUENOS AIRES - DNSSEC para Todos
Lunes, 18 de noviembre de 2013 – 17:00 a 18:30
ICANN – Buenos Aires, Argentina

JULIE HEDLUND: Bienvenidos a todos a esta sesión titulada DNSSEC (Extensiones de Seguridad del Sistema de Nombres de Dominio) para Todos: Una Guía para Principiantes. Por favor, a medida que vayan ingresando, acomódense en la gran mesa rectangular. Deseamos tenerlos a todos al frente para que podamos darles participación en nuestras maravillosas actividades de hoy. Créanme, habrá mucha diversión. Por favor, acérquense. Comenzaremos en un momento. Estamos intentando arreglar algo en la cámara. Y probablemente lo que haremos es iniciar brevemente con la primera parte. Les mostraré las diapositivas y luego continuaremos.

PRESENTADOR: Hola a todos. Ahora comenzamos. Originalmente íbamos a filmar esto con la cámara, pero aparentemente hay cuestiones técnicas que resolver, de modo que por el momento nos saltearemos eso. Estamos seguros que las cuestiones de la cámara no están relacionadas con las DNSSEC, pero dado que algunas de estas cosas con complejas... quien sabe... Esta es la Sesión de DNSSEC para Todos, también conocida como DNSSEC para Principiantes. Esto de las DNSSEC puede ser algo intimidante. Es bastante complejo y técnico. Tiene muchos términos o palabras específicas de moda que suenan importantes y cosas así.

No vamos a poder hacerlos expertos en DNSSEC, pero al menos podrán obtener una introducción general al tema. Al final de esta sesión, al

menos podrán utilizar algunas de las palabras de moda y la gente no se les reirá tanto... Antes de comenzar, permítanme introducir a algunas de las personas que estarán participando en la representación teatral que tenemos.

Tenemos a Russ Mundi, que es el científico principal de redes de *Parsons*. Su grupo hace las herramientas de DNSSEC y él ha estado involucrado en esto durante mucho tiempo. Ha estado organizando muchos talleres y cosas por el estilo. A su lado está sentado Roy Arens. Roy es un becario en investigación y miembro de *Nominet*, que es el registro de .uk; Roy también fue parte instrumental en la creación de una serie de especificaciones de DNSSEC, escribió algunas de las RFCs (Solicitudes de Comentarios), etc.

Al lado tenemos a Julie. Julie ayuda a organizar esto y lo mantiene exacto de alguna manera. Más allá está Norm. Norm es el director de inteligencia del DNS (Sistema de Nombres de Dominio) de *Crowdstrike*. Ellos son una compañía de seguridad informática. ¿Quién me falta? Jaques, que trabaja para CIRA (Autoridad Canadiense de Registración en Internet), que es el registro de .ca, y creo que ahora sí los presenté a todos. En algún lugar también tenemos al Dr. Malvado, pero nadie sabe realmente donde está.

DR. MALVADO: [Risa malvada]

PRESENTADOR: ¡Oh, vaya! ¿Cuántas personas aquí conocen algo acerca del DNS? ¿Podrían por favor levantar la mano? Bien. ¿Cuántas personas aquí

conocen algo acerca de las DNSSEC? Bien. Bueno, lamento decirles que probablemente lo que sepan acerca de la historia está equivocado. Sí. Probablemente piensen que fue inventado hace 10 o 15 años. Y en realidad, fue originalmente inventado hace aproximadamente 7000 años, y fue inventado por un grupo de hombres de las cavernas.

Este es uno de ellos, bueno, una mujer de las cavernas. Su nombre es Ogwina. Y vive en el límite del Gran Cañón. Aquí está otro de los inventores. Su nombre es Og. El vive del otro lado del Gran Cañón. Ogwina y Og tienen algo como un asunto entre ellos. Llamémoslo así. Desafortunadamente, es un largo trecho para bajar al Gran Cañón y un largo trecho para dar la vuelta a él, de modo que Ogwina y Og no se ven tanto como quisieran.

En una de las extrañas visitas, se están mirando amorosamente a los ojos, y notan el humo que está saliendo del fuego de Og. Y no tardaron en darse cuenta que podían utilizar señales de humo para comunicarse entre sí, y que de ese modo podían enviarse cartas de amor entre sí y coordinar inversiones, almuerzos y cosas por el estilo.

Pero sucedió que un día, un hombre maquiavélico de las cavernas, llamado Kaminski, se mudó como vecino de Og. Kaminski cree que es de algún modo divertido insertar mensajes aleatorios entre las conversaciones de Ogwina y Og. Og le estará diciendo a Ogwina cuánto la ama, y Kaminski comenzará a hablar de bananas o de algo que no tenga nada que ver con ello. La pobre Ogwina, ella realmente está confundida. No tiene manera de saber cuáles son los mensajes correctos y cuáles están siendo inventados e insertados por Kaminski.

Y un día se enoja con Og. Así que se da toda la vuelta al Gran Cañón, y camina durante tres días, se va hasta la otra punta opuesta del otro lado, y Ogwina y Og tratan de descifrar qué pueden hacer. Acuden a los ancianos de la villa y les piden asesoramiento. Ellos desean alguna forma en que puedan conversar sin que Kaminski interfiera entre ellos. Uno de los hombres de las cavernas se llama Diffy. El se sienta allí, piensa y pondera el problema.

Y de repente tiene una idea brillante. Se pone de pie y corre a la cueva de Og. En la parte de atrás de su cueva existe esta arena realmente especial. Una de las cosas que hace que la arena sea especial, es el hecho de que únicamente se puede encontrar en la cueva de Og. Diffy toma un puñado de esta arena, corre hacia el fuego de Og y la tira al fuego. Y el fuego se convierte en un fuego azul brillante. Ahora Ogwina y Og pueden continuar teniendo sus conversaciones tranquila y felizmente. Ogwina sabe que todo lo que necesita hacer es únicamente prestar atención a las señales que son azules, porque solamente Og es quien puede colorearlas de esa manera. Kaminski puede sentarse allí e intentar insertar mensajes, pero Ogwina sabe que lo único para hacer es ignorarlos.

Si sacan algo de esta pequeña sesión, es que lo que las DNSSEC hacen es ofrecer el humo de color azul para el DNS. Brinda una manera para que el destinatario conozca que la persona que está enviando el mensaje es una persona que aparenta ser la persona que lo envió. Sólo una persona puede insertar el humo azul, de modo que el destinatario puede determinar cuáles son los mensajes correctos y cuáles no lo son. Dicho esto, le paso la palabra a Roy para que ofrezca una breve presentación sobre la parte del DNSSEC.

ROY ARENS: Hola a todos. Mi nombre es Roy Arens. Y les voy a hablar un poco acerca del DNS y un poco acerca de las DNSSEC. Y en primer lugar quisiera que me muestren las manos. Sé que hicimos esto antes, pero lo preguntaré de una manera algo diferente. ¿Quién de ustedes entiende que tenemos servidores raíz en el mundo? Bien, eso está bien. ¿Quién entiende a un nivel básico cómo funciona el DNS? Lo que es delegado desde la raíz hacia abajo, etc... Bien.

Este es su árbol de DNS estándar. En la parte superior tenemos a la raíz. La raíz delega cosas a .uk, .com, .ar y debajo de ellos están los dominios de segundo nivel: nic.ar, etc. Un resolutor del ISP (Proveedor de Servicios de Internet) o el resolutor de su empresa, básicamente sabe dónde están los servidores raíz. El usuario Joe, que lo presentaremos más adelante, no tiene idea de cómo es el DNS. Joe sólo puede hablar con el ISP. El ISP luego irá desde la raíz, todo el camino hasta el nivel al que se desea llegar, por ejemplo, bigbank.com.

El resolutor obtiene la dirección y esa información se almacena en la memoria caché para su uso futuro. En este momento me gustaría mostrarles cómo hacemos realmente el DNS. Esta es una pequeña representación teatral, una pequeña obra. Y tenemos algunos actores aquí. La diapositiva que vieron antes tenía a los servidores raíz, a los servidores de .com, tenía a bigbank.com, etc., etc. Mientras que el equipo está seleccionando su utilería, les presentaré al usuario Joe. Norm será el usuario Joe. Es el usuario típico. Está sentado en su ordenador portátil, en su sistema, en casa, tratando de navegar hacia alguna parte.

Escribe con el teclado algo en la barra de URL, en la barra de direcciones de su navegador, y todo lo que vamos a mostrarles aquí es lo que básicamente sucede después de que presionan "enter" y antes de ver la página que buscan. Aquí sucede en milisegundos, pero les mostraremos lo que sucede bajo el agua. Para ser justos, eso sucede con los ordenadores y los sistemas, no con la gente de verdad, porque entonces seríamos mucho más rápidos.

Así que tenemos al usuario Joe por allí. Tenemos a nuestro ISP por aquí. Aquí tenemos al servidor raíz. Yo soy .com y esto es bigbank.com. Lo que verán ahora es la manera en que típicamente actúa un resolutor. Pasaré el micrófono a Jaques Latour.

USUARIO JOE: Estoy haciendo bancos en Internet. Tengo que pagar mis facturas. No sé nada acerca del DNS pero no me importa. Lo único que sé es que todos los meses le tengo que pagar al Sr. ISP para tener mi acceso, y él se ocupa de todo. Tengo que pagar las facturas. Me siento en mi computadora y escribo www.bigbank.com.

ISP: Gracias usuario Joe. Yo soy ISP. Acabo de iniciarme, así que básicamente no se nada. Lo único que sé es donde está la raíz. Esto es lo único que tengo programado al iniciarme. No sé dónde está el banco, así que se lo preguntaré a la raíz. ¿Sabes donde está bigbank.com?

RAÍZ: No, disculpe, pero no sé donde está bigbank.com. Sin embargo, sé donde está .com; .com vive en 1.1.1.1. Puede ir allí y preguntarle.

ISP: Muchísimas gracias. Hey, .com! Estoy buscando a www.bigbank.com ¿Usted sabe donde lo puedo encontrar?

.COM: No, no sé donde está www.bigbank.com, pero sé donde está bigbank.com y vive en la dirección 2.2.2.2.

ISP: 2.2.2.2. Hola bigbank, estoy buscando a www.bigbank.com. ¿Usted sabe donde está?

BIGBANK: Bueno, de hecho, sí sé donde está www.bigbank.com. Se encuentra en 2.2.2.3.

ISP: Muchísimas gracias. Hey usuario Joe, la dirección para bigbank es 2.2.2.3. Buena suerte.

USUARIO JOE: Impresionante. Así que ahora he escrito la dirección web del sitio de mi banco. El ISP recibe el número en respuesta y mi computadora lo emite para que pueda hacer mis trámites bancarios. Así que básicamente así es cómo funciona una transacción del DNS. En la vida real lo hace un

poquito más rápido, pero así es como básicamente ocurre una transacción. Sí, ahora la respuesta está guardada en la memoria caché, como lo pueden ver en su panza.

Ahora, lo que en realidad vamos a hacer es mostrarles cómo se ve un hombre en un ataque intermedio. Porque en realidad esta es la motivación detrás de las DNSSEC. Les mostraremos cómo se ve el ataque, nuevamente utilizando maravillosos actores. Ahora repetiremos la misma escena, sólo que esta vez incluirá el ataque intermedio. Aquí vamos. Yo me voy a sentar y a hacer algunos trámites bancarios más. Facturas, facturas, facturas. Escribo en mi teclado: www.bigbank.com.

ISP: Gracias usuario Joe. ¿Deseas ir a Bigbank? Necesito encontrar dónde queda. Primero le tengo que preguntar a la raíz. ¿Usted sabe donde está www.bigbank.com?

RAÍZ: Lo siento Sr. ISP. Pero no sé donde está www.bigbank.com. Todo lo que sé es dónde encontrar a .com. Se encuentra en 1.1.1.1.

ISP: Gracias. Hola Sr. .com. Estoy buscando a www.bigbank.com. ¿Usted sabe donde está?

.COM: No sé donde está www.bigbank.com, pero sé donde está bigbank.com. Bigbank.com vive en 2.2.2.2.

ISP: Muchísimas gracias. Hola bigbank. Estoy buscando a www.bigbank.com. ¿Tiene una dirección IP para encontrarlo?

DR. MALVADO: Oh sí la tengo. La dirección es 6.6.6.6.

ISP: Maravilloso, muchísimas gracias. Usuario Joe, aquí está la dirección. 6.6.6.6. Allí es donde tienes que conectarte para hacer todos tus trámites bancarios.

USUARIO JOE: El idiota. Gracias Sr. ISP, usted estuvo fantástico. Nuevamente, creo que iré a bigbank.com. El Dr. Malvado ha inyectado su propia dirección y ahora me tiene. Mis trámites bancarios ahora se dirigen al Dr. Malvado. Y él se queda con todos mis $3.55c. Como estábamos hablando antes, esta es la forma en que el DNS funciona sin las DNSSEC. Existe tal cosa como un hombre que hace un ataque intermedio, y le ha ocurrido a bancos muy importantes.

Pero parte del problema aquí es que no existe un elemento de conocimiento entre los diferentes servidores aquí en este árbol; en la jerarquía. Ellos no comparten la información, no se hablan entre sí, ni siquiera se conocen entre sí.

Y si recuerdan la comedia acerca del humo azul, hay un concepto que se llama cadena de confianza. Así es como los servidores autoritativos

comparten información y comparten claves, pero eso es como si compartieran el humo azul. En caso de utilizar la cadena de confianza...

ROY ARENS: Antes de pasar al próximo acto teatral, hay algunas cosas que necesito contarles. ¿Recuerdan cuando teníamos a Ogwina del lado izquierdo, conversando con Og? En términos del DNS, en el lado izquierdo está esta hermosa mujer que se llama Ogwina, ella es el resolutor. Ogwina es una mujer moderna. Ella no sólo está conversando con Og, el servidor, sino con muchos Ogs diferentes, es decir, muchos servidores diferentes.

Como saben, Ogwina realmente no sabe quién es el verdadero Og. El resolutor, en este caso, realmente no sabe quién es el servidor real, porque toda esta información que va y viene podría haber sido burlada. Con las DNSSEC, y se los mostraremos en un minuto, Ogwina ahora es capaz de distinguir entre el Og falso, un servidor falso, información falsa, y el Og verdadero.

Ella hace esto con el humo azul. En el mundo del DNS hacemos eso con las claves y firmas del DNS, etc. En realidad no hay seguridad en el DNS. Este protocolo fue inventado alrededor de 1982, 1983. De modo que fue mucho antes de que exista la web. En ese momento, un montón de investigadores, un montón de redes se unieron juntas, pero realmente nadie pensó acerca del uso indebido. En este caso, no hay seguridad, estos nombres son fácilmente burlados y dado que el DNS tiene este concepto de guardar en la memoria caché, esta información burlada no se guardará en ese caché. Se llama partición del caché ('*cached portioning*')

En un minuto haremos el acto teatral nuevamente. En este caso teníamos a la raíz y a .com, al bigbank.com original a la izquierda y al bigbank.com falso a la derecha. Por eso está en rojo, porque el rojo es malo. ¿Cómo hacemos esto con las DNSSEC? Las DNSSEC utilizan el concepto de firmas digitales. Básicamente, se crea un par de claves donde hay una clave pública y una clave privada. La clave pública es algo que puedes darle a quien quieras. La clave privada es algo que almacenas en algún lugar secreto y seguro.

Básicamente la clave pública no es más que un montón de bits, y dado que en el DNS se puede almacenar cualquier cosa, como una dirección —si lo que se desea es buscar una dirección y solicitarla luego—, también se pueden almacenar claves en el DNS y esa es la razón por la cual las llamamos claves del DNS. La clave pública es algo que se puede almacenar en el DNS. Cuando usted firma una DNSSEC, crea algo que se llaman firmas. Lo hace mediante una clave privada, de modo que el mundo que tiene las claves públicas puede validar o verificar eso.

Estas firmas no son más que un montón de bits que también pueden ser almacenados en el DNS. Ahora tenemos las claves del DNS en el DNS y ahora tenemos las firmas en el DNS. Necesita haber un enlace, y les mostraré eso en un segundo, entre todas estas entidades: la raíz, .com y bigbank.com. Básicamente el pegado entre la raíz y .com, y el pegado entre .com y bigbank.com es algo que se llama registro del Firmante de Delegación (*DS record*). Eso no es nada más que la versión simplificada de la clave del DNS.

La clave del DNS de la raíz, la que tiene todo el mundo, necesita estar en un resolutor para que el resolutor confíe en la información que proviene

de la raíz. Dado que ahora el resolutor confía en la raíz, y la raíz ha firmado la información sobre .com, entonces ahora el resolutor también puede confiar en .com.; .com ha firmado información sobre bigbank.com, por lo que el resolutor ahora también puede confiar implícitamente en bigbank.com y así sucesivamente.

En ese mismo concepto de alto nivel, y dado que hemos firmado toda esta información y tenemos esta cadena de confianza desde la raíz hasta .com para bigbank.com, ahora podemos distinguir adecuadamente entre la información falsa que no puede ser debidamente firmada, porque el atacante no tiene la clave privada que bigbank.com tiene; y ahora el resolutor puede distinguir adecuadamente entre la información debidamente firmada y la información sin firmar o falsamente firmada.

Ahora haremos el acto teatral con las DNSSEC vigentes. Todo lo que acabo de decirles, lo aplicaremos al acto teatral que acabamos de hacer. ¿Puedo invitar a mis amigos nuevamente?

RAÍZ: Hola a todos. En primer lugar la raíz debe estar firmada. Así que me firmaré a mí mismo. Hey, miren todos, esta es mi clave. Ahora necesito intercambiar claves con .com. Hola, ¿tú realmente eres .com?

.COM: Sí, realmente soy .com.

RAÍZ: En ese caso, podemos intercambiar claves.

.COM: Gracias.

ROY ARENS: Básicamente este es el intercambio de claves. Lo que acabamos de hacer, lo haremos nuevamente aquí.

.COM: Hola, soy .com. ¿Puedo confiar en que eres bigbank.com?

BIGBANK.COM: Yo soy bigbank.com.

.COM: Perfecto. Mereces una estrella. Bien hecho Russ.

ISP: Ahora tengo toda mi zona firmada de modo que la dirección www.bigbank.com está firmada.

USUARIO JOE: Ahora vamos a hacer nuevamente una transacción del DNS, hacemos lo mismo, nuevamente el hombre ataca en medio de la transacción, pero esta vez tenemos a las DNSSEC como protección. La misma transacción, más facturas. En realidad ya no me queda dinero, porque la última vez me estafó el Dr. Malvado. Hora de hacer bancos. www.bigbank.com. ¿Sr. ISP?

ISP: Gracias. ¿Deseas ir a www.bigbank.com? No sé dónde queda, así que lo preguntaré por aquí. Ahora necesito hablar con la raíz. IANA (Autoridad de Números Asignados en Internet) publicó la clave pública para la raíz y ellos la validaron, y yo sé que es la raíz. ¿Sabes donde está bigbank.com?

RAÍZ: Sí, lo sé. Bigbank.com está en 1.1.1.1. Dame un segundo, déjame firmar esto por ti.

ISP: Bien. Revisé la firma que me ha dado. Y la firma coincide con su clave. Estamos bien. Muchísimas gracias. Tengo que hablar con 1.1.1.1.

RAÍZ: Cuando hable, su clave es... Y aquí hay un número realmente largo.

ISP: Gracias. 1.1.1.1, hola .com, deseo ir a www.bigbank.com, ¿sabes dónde está?

.COM: No sé donde está www.bigbank.com, pero sé donde está bigbank.com. Bigbank vive en la dirección 2.2.2.2. Aquí hay una firma sobre esa información, y aquí también está la clave para bigbank.com

ISP: Las claves están verificadas, la firma, revisa.... Todo está bien. Perfecto, todo bien. Le preguntaré a bigbank.com por www.bigbank.com.

DR. MALVADO: Yo sé la respuesta. La respuesta es 6.6.6.6.

ISP: Muchísimas gracias. Déjeme revisar la clave. La clave no funciona... Hey! ¡Lárgate de aquí! Muchísimas gracias. La dirección es....

BIGBANK: La dirección es 2.2.2.3 y está firmada.

ISP: Necesito verificar eso... Perfecto, muchísimas gracias. Usuario Joe, tengo la dirección. Es 2.2.2.2 y las firmas son válidas.

USUARIO JOE: Estupendo. Muchísimas gracias ISP. Ahora tengo una resolución validada hacia este número y así es como funciona la transacción. Un punto importante aquí, ustedes notarán que yo, como usuario Joe, no tenía nada. Yo sólo hice la misma solicitud y todo pasó en los servidores, la raíz y el ISP, los registros y los registradores y los titulares del dominio. Pero no colocó ninguna carga sobre los usuarios para hacer todo eso.

Eso es todo. Gracias. Dr. Malvado, realmente le tiene que gustar eso.

PRESENTADOR: Bien, muchas gracias a todos. Realmente intentamos que esta sea la sesión más divertida de la semana. No sé si tenemos éxito o no, pero realmente lo intentamos. Nosotros en verdad deseamos mantenerlo informal, de modo que hasta el momento no se han planteado preguntas, pero esta es una sesión muy informal así que si algo viene a la mente que deseen sea contestado, por favor griten, levanten la mano, lo que sea e intentaremos detenernos y abordarlo en ese momento o decirles exactamente de cuándo viene.

Mi parte aquí en la presentación de esta sesión es hacer dos cosas: darles un ejemplo más específico de un secuestro y de aquello que puede ser el resultado real de uno.

JAQUES LATOUR: Ya tengo una pregunta en base al pequeño acto teatral que acaban de hacer. Vi a una persona que tenía un fuerte acento francés haciendo todo esto en inglés. ¿Es el mismo caso en que realmente se necesita usar el idioma inglés para las DNSSEC o también se aplican para las cadenas de caracteres internacionalizadas?

ROY ARENS: Gracias. Funcionará, y fueron diseñadas para funcionar con cualquier información que esté contenida en el DNS. Si se trata de datos del DNS en cualquier otro conjunto de caracteres de escritura, desde la perspectiva del DNS sólo se trata de bits. Funcionará si tiene otros idiomas que utilice en su procesamiento normal. Estupendo, gracias. Pasemos a la primera diapositiva porque tuvimos el acto teatral hasta

aquí sobre las DNSSEC y vimos por qué es posible que ustedes se preocupen por ello.

La conclusión de todo esto es que el contenido del DNS en sí mismo necesita obtener correctamente las aplicaciones que van a utilizarlo, o sucederán cosas malas e inesperadas. En realidad lo que más les preocupa es realmente la aplicación del usuario final. Los usuarios finales realmente creen que la mayor parte del DNS, se trata sólo de los nombres.

Sin embargo, la infraestructura de red subyacente y la mecánica de dicha estructura, todos utilizan las direcciones IP de un tipo u otro, de modo que hay que obtener esta traducción en forma correcta. Allí es donde el secuestro toma lugar, en términos de cambiar las direcciones IP reales que usted va a utilizar por mecanismos que distorsionarán los bits. Esa es realmente otra forma de describir lo que es un secuestro de DNS.

Al hacer un secuestro del DNS, no es realmente para secuestrar el DNS para beneficio del DNS. A nadie le importa realmente. El DNS es importante para los fanáticos informáticos del DNS, pero las personas que realmente trabajan en Internet se preocupan por sus aplicaciones, y esa es la gente hacia la cual los secuestros están orientados. Así que una de las cosas que me pareció sorprendente —hace unos cinco años, cuando me topé con esto— es que hay software abiertamente disponible que permite realizar un secuestro de DNS, y está disponible en Internet.

He encontrado un par de universidades que en realidad requerían, como parte de su curso de informática, que los estudiantes escriban un

software que hiciese un secuestro del DNS. Y hablando de eso... Desconozco cuántas cosas de uso ético ellos asociaban al tema, aunque no vi muchas; pero pensé que era lamentable que en realidad estuviesen presionando para escribir un código que realmente hiciese esto. Hay una gran cantidad de códigos que existen por ahí y es algo que obviamente los estudiantes universitarios pueden hacer, porque se les ha pedido.

Cuando en realidad van a hacer uso del DNS y las DNSSEC en un sitio web, pueden utilizar la información que es parte del protocolo para hacer cosas que ayuden a la gente a ver si están o no están haciendo uso de las DNSSEC cuando llegan a esos sitios web. No se hace muy a menudo, pero hay algunos sitios que lo hacen, y por supuesto, algunos de los lugares asociados con... Son proyectos que tienen esta capacidad.

Lo que hicimos es: modificamos... parte de nuestro sitio web para que en realidad pueda mostrar una verdadera demostración en vivo del secuestro de parte de una página web. Esta diapositiva muestra cómo los paquetes reales están volando alrededor, que es una imagen diferente, pero más o menos lo mismo que acabamos de mostrarles en el acto teatral. Lo que sucede es que el usuario Joe envía su consulta al resolutor local del ISP y se inicia la búsqueda de un lado a otro de la red y, finalmente, consigue la respuesta de vuelta.

Después de retornar la respuesta, es cuando la máquina del usuario Joe es realmente capaz de hablar con el banco. La aplicación en realidad no puede hacer lo que el usuario está queriendo hacer hasta que obtiene la respuesta completa devuelta por el DNS. Cuando se tiene un navegador

consciente de las DNSSEC, el sitio en particular que estaba describiendo anteriomente está en despliegue-de-DNSSEC.com.

Se puede ver en el navegador superior, donde se indica la marca de verificación de DNSSEC; y podemos detectar eso al observar cómo las consultas del DNS entran en ese sitio en particular, y si tiene las capacidades de DNSSEC y está haciendo las preguntas correctas y el procesamiento apropiado de las respuestas. Le daremos una marca de verificación del DNS. Si su navegador no tiene eso, usted obtendrá un "DNSSEC desactivadas". Sólo un pequeño indicador para decirle al usuario que está mirando una página que tiene las DNSSEC activadas o desactivadas.

Aquí está el Dr. Malvado secuestrador, que es el equivalente al Dr. Malvado. A medida que la consulta es enviada por el usuario Joe, el Dr. Malvado observa cuál es la petición, a través de alguna forma que le permite hacerlo, y estando en el lugar correcto es bastante fácil de hacer. Entonces eso hace el Dr. Malvado, y en segundo lugar, obtiene la respuesta que va al usuario Joe antes de que la respuesta real llegue. En esta ilustración pueden ver que va mucho más allá. La respuesta real toma un poco más en regresar que la respuesta falsa.

Ahora, si se están usando las DNSSEC tal como se vio en la obra de teatro, lo que pasa es que el usuario Joe es capaz de detectar que la respuesta que recibe del Dr. Malvado secuestrador no es válida, de modo que ignora esa respuesta y obtiene la respuesta adecuada enviada a partir de las DNSSEC para la ubicación real, y entonces puede llegar al servidor web que realmente desea llegar.

Esta es otra forma de ilustrar lo que acaban de ver en el acto teatral. No coloqué todo lo de la raíz y todo lo de .com porque al incluir todas esas máquinas la diapositiva se vería congestionada. ¿Alguien tiene alguna pregunta? ¿Si?

HOSAM HASSAN: Soy de Egipto. Y en realidad tengo una pregunta y he escrito [inaudible 00:39:30] no puedo obtener una respuesta a mi pregunta relacionada con el DNS y las DNSSEC.

ROY ARENS: Lo siento, no puedo escucharle. ¿Podría acercarse un poquito por favor?

HOSAM HASSAN: En realidad, las DNSSEC construyen la relación de confianza entre la raíz y el otro dominio de nivel superior, por ejemplo .com y otros dominios, pero si el caso es que el secuestro ocurre en el resolutor en sí mismo o en el ISP o en el usuario final, si el usuario final está utilizando su propio DNS. Sé que el resolutor contiene las direcciones de los servidores raíz, de modo que si el secuestro ocurre en esta etapa y apunta o enruta el tráfico a otro servidor raíz que está fuera de ese alcance, entonces las DNSSEC no tienen nada que ver con esto. ¿Se entiende mi pregunta?

ROY ARENS: Creo que entiendo lo que está preguntando. Si puede terminar como un operador del resolutor que está trabajando para usted y utiliza una ruta diferente que no tiene las DNSSEC firmadas...

HOSAM HASSAN: No, no. Vea, tal como lo he visto, la relación es entre la raíz, .com y niveles debajo de los dominios. Aquí está el resolutor. El...el secuestro ocurrió en el resolutor en sí mismo o en el ISP en sí mismo, antes de salir de la raíz.

ROY ARENS: si la pregunta en sí misma es modificada…

HOSAM HASSAN: En el resolutor en sí mismo. Para señalar a una dirección IP fuera de los servidores raíz, la dirección IP sin embargo, su servidor u otro servidor, estaría fuera del ecosistema del dominio. Irá a otro servidor que puede contener otro servidor raíz en el camino.

ROY ARENS: Creo que... Sí, adelante Russ.

RUSS MUNDY: Primero voy a repetir la pregunta en la forma en que creo haberla entendido. Me disculpo de antemano si lo entendí equivocadamente, lo cual es altamente probable. La manera en que entiendo su pregunta es: ¿qué sucede si la pista de la raíz en el resolutor de ISP está comprometida; comprometida de una manera en que las direcciones IP están cambiadas para apuntar a un tipo de servidor completamente diferente y no los servidores raíz de la ICANN?

HOSAM HASSAN: Exactamente. Esa es mi pregunta.

RUSS MUNDY: Mi respuesta a eso es, si la pista de la raíz está comprometida pero el resolutor aún es capaz de hacer la validación, debido a que cuenta con la clave del DNS, si tiene la clave del DNS seguirá intentando validar esa información de la raíz. Como se trata de una raíz alternativa, la información es obviamente errónea y la validación fallará. Eso significa que la información no irá al usuario final.

HOSAM HASSAN: No, no. En realidad el secuestro sucede en el resolutor del ISP, antes de que las DNSSEC sean activadas. Las DNSSEC se activan entre el TLD (Dominio de Nivel Superior), el servidor raíz y el servidor del nivel subyacente, pero cuando se inicia el tráfico desde el ISP, el mismo apunta a una base de datos o a un servidor fuera del alcance del DNS, otra base de datos, otro ecosistema, otra base de datos del DNS; en esa etapa las DNSSEC no tienen nada que hacer con eso y el secuestrador puede apuntar a otro. En un clic la dirección de IP es 6.6.6.6 en lugar de todo este viaje.

RUSS MUNDY: Permítanme señalarlo un poco aquí. El resolutor del que estamos hablando es el que se encuentra aquí, en la parte superior: 10.1.1.253. Ahí es donde el usuario Joe está enviando su primera consulta, son los ISPs. Si cualquiera de la maquinaria de la cadena del DNS en realidad está significativamente comprometida a partir de un software que se ejecuta correctamente en ese equipo, los resultados son totalmente

impredecibles. De estar comprometida, ellos pueden hacer cualquier cosa por cambiar cualquier cosa.

Usted tiene que tener la confianza de que su ISP está funcionando apropiadamente o no. Además, el punto de tener confianza en una operación profesional es que ellos deben hacerlo bien. Las DNSSEC no pueden garantizar los requisitos de seguridad de su equipo, sus necesidades físicas, sus otros requisitos de protección serán cumplidos y deben ser cumplidos en forma adicional a las DNSSEC, para poder funcionar en forma alineada a las DNSSEC. Warren, ¿deseabas añadir algo?

WARREN KUMARI: Gracias. Warren Kumari de Google. Sí, si usted no confía en los resolutores de su ISPs o si los resolutores de su ISP no son dignos de confianza, ellos le pueden mentir. Hay una cantidad de personas que han escrito software para que usted pueda ejecutar su propio resolutor localmente, en su ordenador. El software Unbound, por ejemplo.

HOSAM HASSAN: El usuario final puede usar esto en el DNS o en el resolutor del ISP.

WARREN KUMARI: Sí, y creo que el ejecutar algo como el Unbound localmente en su ordenador es una muy buena idea, porque de esa manera se puede evitar la necesidad de confiar en su ISP. Usted no tiene que confiar en nadie que no sea su propio ordenador.

RUSS MUNDY: De hecho, si se fijan en los navegadores que utilizo aquí en la ilustración, el propio navegador en sí mismo es el que hace la validación de las DNSSEC. Eso es lo que tengo en mi máquina, y estoy seguro que la mayoría de estos chicos tienen algo equivalente en sus máquinas. No es esencial confiar en su ISP. La mayoría de la gente podría hacerlo más fácilmente y confiar más rápidamente en su ISP, y van a depender de su ISP para un montón de cosas. De modo que confiar en ellos para hacer la operación segura y apropiada es una cosa más, aunque no es esencial para el éxito de las DNSSEC. ¿Aborda eso lo que estaba preguntando?

HOSAM HASSAN: Aborda el tema pero en realidad, para ser honesto con usted, hasta el momento no encontré la respuesta correcta; desde mi perspectiva de cómo asegurar al usuario final en el punto de vista de la resolución, no del ciclo de vida de las DNSSEC.

JULIE HEDLUND: Russ, ¿podría sugerir que continuemos adelante? Creo que habrá cierta cantidad de preguntas. ¿Deberíamos tal vez pedirle a la gente que reserve sus preguntas hasta el final de la presentación?

RUSS MUNDY: Sigamos adelante y hagámoslo. Pasemos a la siguiente diapositiva. Esto no tomará demasiado tiempo más. Ahora, en la parte superior verán lo que ahora se llama el navegador Bloodhound, ese es su nombre. Es un derivado de Firefox, Mozilla y tiene la capacidad de DNSSEC completa de modo que hizo toda la comprobación y el secuestro estaba pasando. La información secuestrada no está presente allí.

Nuevamente, este es su navegador normal y es literalmente —si nos fijamos en la barra de URL en la parte superior—, fueron enviados al mismo lugar y estaban solicitando la misma información. Pueden ver que el navegador que no tiene DNSSEC recibió la información de secuestro señalando que Steve Crocker finalmente admite que las DNSSEC no acabarán con el hambre en el mundo. En este caso la intención es que sea algo muy obvio y tonto, es algo que no es real, pero eso era del secuestro. Eso es contenido específicamente insertado a partir de un secuestro del DNS.

Ahora, miran la página web y dicen: "Oh, sólo está la barra de URL en la parte superior". Esta es una imagen de cuántas consultas al DNS tomaba completar su sitio web estándar comercial, hace cinco años. Eso es lo que toma hoy en día. El completar cnn.com toma una enorme cantidad de consultas. Nuevamente, lo importante aquí es llegar a los datos de zona correctos y de eso se tratan las DNSSEC. La criptografía es un mecanismo esencial para garantizar que eso suceda, pero son los datos de zona en sí mismos lo que realmente constituyen la información crucial que usted desea conseguir en el lugar adecuado en el estado adecuado, y que sea la correcta.

Aquí hay otra imagen que simplemente muestra lo que ocurre. No voy a profundizar sobre el flujo de datos, pero es otra respuesta a la consulta como la que vimos antes. Por supuesto, estas diapositivas se encuentran en el sitio web y si lo desean las pueden ver más tarde o utilizarlas, eso también está perfectamente bien. Esta es su consulta estándar.

Luego, lo que sigue es colocar las DNSSEC en escena. Dependiendo de donde usted se encuentra en toda esta cadena del DNS, usted ha visto un ISP aquí haciendo principalmente de resolutor recursivo. Ha visto a la raíz, ha visto a .com, ha visto a .bigbank y todos tenían diferentes funciones en el ámbito de las DNSSEC. Cualquiera sea su rol para hacer cosas relacionadas con el DNS, la recomendación general es que usted debe hacer el mismo tipo de cosas cuando lo haga con las DNSSEC.

De modo que si usted está haciendo todo en forma interna, porque el DNS es fundamental para cualquiera que sea su misión o función —si usted es un operador de TLD tendrá una experiencia enorme en las DNSSEC—, usted probablemente deba hacer las DNSSEC en forma interna, con la misma gente, dado que cuenta con personal muy bueno, muy altamente calificado y competente.

Si usted es una empresa y está tercerizando otra actividad, probablemente debería tercerizarlo también. Con suerte esa misma actividad será capaz de hacer las DNSSEC, pero si no pueden, entonces debería buscar otra actividad que sea capaz de hacer las DNSSEC para usted de forma tercerizada, a menos que desee desarrollar pericia en DNS dentro de su propia organización.

Sin embargo lo hará si usted es un usuario final y desea utilizar las DNSSEC hoy en día, si usted es un usuario de Mac —que cada vez hay más, y la razón por la cual primero construimos para Mac es que es la plataforma más fácil de construcción para este tipo de cosas—, puede conseguir el navegador Bloodhound ahora mismo, hoy, y puede ejecutar las DNSSEC en su máquina de usuario final como navegador por defecto, y puede ejecutar DNSSEC ahora mismo, hoy, usted mismo, fácilmente.

Respecto a los datos de zona, las DNSSEC son lo que le ofrece esa garantía. Es lo que, en palabras finales, ingresa al DNS mediante las personas autorizadas para colocarlas en una zona, es lo que las DNSSEC le indican que está obteniendo en el lugar en que usted está haciendo la validación. Ya sea que se trate de su máquina de usuario final o de su ISP. En los Estados Unidos, un gran proveedor de cable llamado *Comcast* está haciendo la validación de las DNSSEC en todos los resolutores, para algo así como 18 millones de clientes. Una base enorme, un ISP muy grande, y están haciendo la validación de DNSSEC del tipo de ISP.

Y aún usted lo puede hacer en sus resolutores de usuario final. Yo soy cliente de *Comcast* y también lo hago en mis resolutores finales. Oh sí, gracias Warren. Google... Para cualquiera, en cualquier lugar del mundo, 8.8.8 y 8.8.4.4 están haciendo la validación de DNSSEC. De modo que si lo desean pueden utilizar la validación de DNSSEC ahora mismo. El enlace entre el validador y su máquina final no tendrá ninguna seguridad particular, pero usted también puede utilizar las DNSSEC utilizando los validadores de Google.

Al activar las DNSSEC, y esto es una ilustración simplificada, pero en realidad todo lo que necesita hacer es obtener los datos firmados, y entonces usted necesita lograr que se validen en algún lugar, ya sea en su máquina o en el servidor recursivo de validación. Esto lo muestra en el servidor recursivo, podría también ser en la máquina final. Nuevamente, el principio general...Sí, ¿Olaf?

OLAF KOLKMAN: Sólo para ponerle un número, Feoff Huston del APNIC (Centro de Información de Redes de Asia Pacífico) hizo algunas investigaciones y

observó la cantidad de la población de muestra que estaba protegida por las DNSSEC y el tamaño de esa población. Este es un experimento a nivel mundial. El 8% de los usuarios de navegadores en Internet están protegidos por las DNSSEC. Eso mayormente se debe a la infraestructura de Google, pero es una cantidad significativa de usuarios de Internet que están protegidos por las DNSSEC desde el lado del cliente.

RUSS MUNDY: Estupendo, gracias. Olvidé acerca de esos números. Sí. De modo que donde quiera que esté haciendo su DNS, cualquiera que pueda ser su operación de DNS, usted debe usar el mismo enfoque general para ejecutar las DNSSEC y garantizar —y esto es un aspecto importante— que cualquiera que sean sus proveedores de software o hardware, usted necesita asegurarse de pedir apoyo de DNSSEC. Durante muchos años ha habido una gran cantidad de proveedores diciendo: "¿Dónde está la demanda?" De modo que la gente necesita solicitarlo.

Si no es así, si no está disponible ahora, este es también un momento para tal vez evaluar el cambio de algunos de sus proveedores o cualquiera que sea la fuente. Ese es el conjunto de información para las presentaciones planificadas. Ahora estamos completamente abiertos a preguntas y comentarios. Yo tengo una pregunta que desearía realizar amigos. Tuve las diapositivas que mostraban un secuestro y describí el secuestro, ustedes vieron el secuestro en la obra teatral.

¿Podrían comentar si desearían o no verlo hacer de verdad? Así podríamos establecer una red inalámbrica y secuestrar su ordenador o secuestrar su ordenador. ¿Sería valioso eso para las personas?

Obtenemos un sí. Bien. Si esto es algo que se desea, veremos de hacerlo en la próxima reunión de la ICANN, como parte de esto, para mostrarle a la gente que esto es real! Bien, ¿alguien tiene algún otro comentario sobre eso? ¿Si?

MIEMBRO DE LA AUDIENCIA: Yo tengo una pregunta, no un comentario. ¿Está el micrófono abierto para preguntas ahora?

RUSS MUNDY: Seguro, adelante.

MIEMBRO DE LA AUDIENCIA: Bien. Mi pregunta es más bien como un usuario final, más que como un becario de la ICANN. Hablando de todas las amenazas y los problemas de seguridad entorno al DNS, yo quisiera saber ¿lo mismo aplica a las aplicaciones? Porque la mayoría de los sitios web de uso frecuente que utilizamos ahora tienen aplicaciones, no vamos a la página web. ¿Las aplicaciones agregan una capa más o es más riesgoso usar las aplicaciones?

RUSS MUNDY: Julie, ¿podríamos volver un par de diapositivas? El navegador que ha visto es un navegador instrumentado para ejecutar DNSSEC. Usted no tiene que tener aplicaciones que reconozcan las DNSSEC, aunque es muy útil si lo hacen, que sean capaces de ver que el contenido... ¿la marca de verificación? Usted tiene que contar con aplicaciones compatibles con DNSSEC. Hay trabajos en curso para una interfaz de programación de

aplicaciones. Ha habido alguna labor sobre eso con el tiempo e intentando conseguirla a través de donde las aplicaciones puedan estandarizarse.

ROY ARENS: Yo interpreté su pregunta ligeramente diferente. No hay ninguna aplicación de navegador, básicamente nada, cosas en su iPhone para que pueda utilizar las DNSSEC. Las DNSSEC son independientes de la aplicación, de modo que si cualquier aplicación utilizara el DNS y su resolutor o el resolutor de su ISP es compatible y capaz de apoyar las DNSSEC, y todo eso está encendido, todas las aplicaciones se beneficiarían a partir de ello. Espero que eso responda a su pregunta.

OLAF KOLKMAN: ¿Puedo darle un giro diferente en esto? Siempre que utiliza Internet, con todo lo que haga en la vida, cómo su organiza tu vida, esencialmente utiliza el DNS —ya sea que se trate de su agenda, de las noticias, de enviar un correo electrónico, un mensaje instantáneo, ya sea haciendo un llamada telefónica a través de Internet—, todo en el back-end utiliza al DNS como recurso para llegar a alguna parte.

Todos estos factores de ataque, todas estas cosas que acabo de mencionar, tienen valor. Las manos también son un factor de ataque. Al activar las DNSSEC, usted introduce una capa adicional de seguridad para aquellas aplicaciones que no son necesariamente las cosas que escribe o utiliza, sino que el DNS utiliza en las transacciones internas. Esa es la misma respuesta con palabras diferentes.

ROY ARENS: Gracias Olaf.

JULIE HEDLUND: Tenemos una pregunta a distancia.

ORADOR: Esta pregunta es de Ade Bumbekimbo. Y es: ¿cómo se despliegan e implementan las DNSSEC en un ccTLD (Dominio de Nivel Superior con Código de País)? ¿Qué se necesita para garantizar que funciona y quiénes son las partes que deben estar involucradas?

ROY ARENS: Bien, en realidad sucede que trabajo en un ccTLD, .uk. Hemos pasado por este ejercicio, pero lo que ha preguntado es una pregunta muy amplia. Si tuviese que responder a eso sería una sesión muy larga. Nada de esto es nuevo. Una gran cantidad de ccTLDs ya han desplegado DNSSEC, hay una enorme cantidad de información allí. Está DNSSEC-2.org, de la compañía de Russ.

Esencialmente, lo que necesita es firmar su zona, almacenar sus claves de forma segura, necesita obtener su registro del DNS en el servidor raíz, necesita hacer una enorme cantidad de pruebas, porque cuando usted firma cosas eso básicamente significa que usted... básicamente tiene a otras personas para autenticarlo, de modo que necesita garantizar que sea correcto.

Así que ya no se trata de una gran ciencia. Tal vez hace diez años era muy difícil hacer todo esto, pero hoy en día hay un montón de herramientas por ahí, existe una gran cantidad de documentos. Russ y

sus diapositivas tienen muchos enlaces diferentes que contienen toda esa información. ¿Quizás Russ quisiera elaborar un poco más?

RUSS MUNDY: Sólo quería señalar algunos cálculos que se están haciendo: aproximadamente una tercera parte de los TLDs han ahora firmado en la zona raíz y sigue creciendo. Su tasa de crecimiento sigue aumentando. Más temprano, mientras hablaba sobre el lugar donde actualmente ejecuta sus funciones de DNS, si usted es un proveedor de TLD, un titular, y está asociado a un registro que es un operador, puede que ya tenga un socio de registro que ya tenga compatibilidad con las DNSSEC.

Podría no ser más complejo que hablarlo con su registro asociado para ver si en la actualidad operan las DNSSEC, y activarlas para su zona. O puede ser, como dijo Roy a partir de cero, sin en realidad tener nada, que planifique y compruebe y garantice que es correcto antes de ponerlo en funcionamiento. ¿Por aquí? Adelante.

MIEMBRO DE LA AUDIENCIA: ¿Se han utilizado DNSSEC para el correo electrónico? El 40% del correo electrónico mundial es correo no deseado (*spam*). Como consultor, trabajo para varias empresas que envían cientos de millones de mensajes de correo electrónico, y el mayor problema es que los mensajes de correo electrónico legítimos son cortados por los filtros de spam. ¿Qué se está haciendo en el mundo de las DNSSEC para ayudar a esta situación? Gracias.

RUSS MUNDY: Bueno, creo que fue Roy quien lo mencionó antes o tal vez fue Olaf, pero cualquier aplicación que esté ejecutándose en una máquina que utiliza DNSSEC se puede beneficiar a partir de ello. Hasta este momento ha habido algunas implementaciones que están específicamente señaladas en SMTP e incluso en IMAP; que son capaces de ver si las DNSSEC han sido o no utilizadas por debajo de ellas. Pero la actividad más reciente que está tomando lugar es algún trabajo en la IETF (Fuerza del Trabajo en Ingeniería de Internet) que utilizaría la tecnología DANE (Autenticación de entidades identificadas basada en el DNS) conjuntamente con las DNSSEC, lo que ayudaría a fortalecer el enlace de SMTP a SMTP. ¿Roy?

ROY ARENS: Para el correo electrónico hay... Para las complicaciones entre MTAs (Agentes de Transferencia de Mensaje) existe algo que se llama DKIM, DMARC, etc. Estos son protocolos que fueron inventados, desplegados, estandarizados, etc.; que eventualmente pueden llegar a hacer uso de cosas como las DNSSEC o algún tipo de mecanismo de seguridad, básicamente, que esté basado en un principio criptográfico. Sin embargo —y me gusta mucho esta cita, aunque no es mía sino de alguien más—, los ladrones de bancos también usan cinturones de seguridad. Las DNSSEC son un tipo de tecnología de cinturón de seguridad. Sólo resuelve partes pequeñas; las partes del DNS.

Si los generadores de spam utilizan los protocolos DKIM de tal manera que eventualmente utilicen las DNSSEC, entonces usted no ha resuelto el problema del spam de esta manera. Espero que esto ayude. ¿Señor?

PAUL DONOHOE: Hola, soy Paul Donohoe de la UPU (Unión Postal Universal). Somos patrocinadores de .post. Hola Russ, nos hemos encontrado antes en Italia, en una conferencia sobre DNSSEC. Gracias por su explicación simple de un tema muy complejo. Tengo un par de cuestiones que quisiera consultarle. La primera es .post es enteramente de DNSSEC, de modo que todos los nombres de dominio en .post tienen DNSSEC firmadas. Es un desafío para nuestra comunidad, particularmente como gTLD (Dominio Genérico de Nivel Superior) realmente estamos haciendo un montón de trabajo en África, América del Sur y Asia para los nombres de dominio.

Nos encontramos con que hay una adopción muy lenta dentro de la infraestructura en esas áreas. Uno de los retos a los que nos enfrentamos, y una de las preguntas que tengo para usted, es ¿cómo conseguir una mayor adopción dentro de la infraestructura en estos países? ¿Qué podemos hacer para alentar la adopción? La segunda cuestión está de algún modo relacionada: ¿cómo, como usuario sentado frente a mi ordenador, me siento más cómodo con un sitio web en el que estoy actualmente? ¿Cómo digo que esto está asegurado en el uso informático general?

Esta es una de las preguntas de muchos de los usuarios de los dominios en .post. Yo les digo: "Estamos usando las DNSSEC, todo está firmado, todo es seguro", pero ¿cómo el usuario final siente esa tranquilidad, siente esa seguridad, si están usando alguno de estos programas generales que están disponibles todos los días? Creo que ese es uno de los desafíos.

ROY ARENS: Intentaré responder eso. Permítame primero repetir su pregunta, y voy a ser un poco más genérico si no le importa. La pregunta es, ¿cómo podemos ayudar a la adopción de las DNSSEC dentro de los dominios de segundo nivel, por debajo, por ejemplo de .post o los nuevos gTLDs?

PAUL DONOHOE: Solo para aclarar que, ya tengo todos los dominios firmados, de modo que es más sobre ¿cómo los dueños de esos dominios tienen acceso a la seguridad de DNSSEC para que esta firma pueda suceder? Ya tengo la infraestructura necesaria en el registro, con mi operador de registro, y estoy pidiendo a la gente que me de los datos del Firmante de Delegación. ¿Cómo obtienen estos datos del Firmante de Delegación? Necesitan ya tener la capacidad en su infraestructura, ¿cierto?

RUSS MUNDY: Ahora, si usted está preguntando acerca de los nombres debajo de .post, para obtener esos firmados ¿o los...? Bien. El operador de registro está listo en .post, pero quien quiera que esté operando el DNS en el siguiente nivel, ya sea un país, lo que imagino en el caso de .post sería muy común. U otra entidad para, digamos, cosas de acuerdos o lo que sea, si no existe un mandato político para ello, la gente es reacia porque es difícil.

Como Roy dijo anteriormente, hay una gran cantidad de herramientas, hay un montón de cosas disponibles que son gratuitas de modo que se convierte en una cuestión de saber acerca de ellas, saber dónde están. Si la gente que es la siguiente etiqueta hacia abajo tiene la experiencia para hacerlo, de cualquier modo que estén operando su DNS en la

actualidad, una tercerización para ellos a otro tipo de operador de servidor de nombres, entonces necesitan averiguar si ese operador del servidor de nombres es capaz de ejecutar las DNSSEC.

Si no lo es, el gran cambio que existe es que lleven su negocio a uno que sí sea capaz de hacerlo. Hay una serie de operadores de servidores de nombres que están intentando generar su modelo de negocio más fuerte porque ejecutan DNSSEC. A menos que haya algún impedimento político, se convierte en una cuestión de ayudarles con la zanahoria en lugar de con el impedimento.

ROY ARENS: También hubo una segunda pregunta. Tal vez en el tema de la primera pregunta, Suecia y los Países Bajos —.se y .nl—, son básicamente los referentes en términos de adopción de las DNSSEC. Lo que ve allí, creo que parte de la razón de su éxito es que hacen un poco de marketing y ofrecen un descuento a quien registra un dominio y despliega las DNSSEC. Ese es un camino a seguir. No estoy seguro de si ese es el camino correcto o equivocado.

Su segunda pregunta fue ¿cómo el usuario final sentado detrás de un navegador se beneficia a partir de todas estas cosas de DNSSEC? ¿Hay un mecanismo de señalización? ¿Cómo puede un usuario ver si está detrás de un resolutor de validación de DNSSEC? ¿Cómo puede sentirse seguro? Actualmente no existe eso en producción. Si usted descarga un navegador o utiliza un navegador estándar con OSX o Windows, no se ve nada. No hay nada allí. Si está desplegado, está mayormente desplegado en los ISPs o por fanáticos informáticos como nosotros, por los TLDs, etc.

Pero hay actualmente actividades en curso para conseguir un mecanismo de señalización y Olaf Kolkman que está por aquí, le he oído decir a él esta tarde algo acerca de un proyecto que está haciendo conjuntamente con un gran TLD con el fin de obtener al menos un estándar de este mecanismo de señalización hacia el usuario. ¿Tal vez podría elaborar sobre esto Olaf?

OLAF KOLKMAN: Sí, puedo hacerlo. He estado interviniendo un par de veces sin haberme presentado a mi mismo. Mi nombre es Olaf Kolkman, trabajo para NLnet Labs y NLnet Labs ha estado trabajando con gente como Russ en una pequeña comunidad por más de una década observando las DNSSEC y el despliegue de las DNSSEC y ver dónde podemos hacer una diferencia. Con respecto a lo que usted acaba de mencionar, lo que nos interesa ahora es específicamente esa última milla ¿cómo hacer llegar las DNSSEC al usuario y cómo se consigue en la aplicación?

La pregunta que acaba de hacer fue básicamente una cuestión de interfaz del usuario. Allí no está nuestra especialidad, pero además esas aplicaciones necesitarán saber si las DNSSEC están siendo utilizadas. Las APIs (Interfaces de Programación de Aplicaciones) actuales no ofrecen esa capacidad, y hay trabajos en curso dentro de la IETF y con un montón de personas que están tratando de desarrollar una API que ofrezca esa capacidad a los programadores. Llegar allí podría llevar algún tiempo.

Pero deseo dar un paso atrás porque tenía un enfoque diferente para responder a su pregunta. Pensé un poco acerca de aquello que se necesita para una innovación de este tipo en una escala global.

Tenemos la misma pregunta con IPv6: ¿cómo innovar en la infraestructura básica de Internet? Ahora bien, si nos fijamos en la innovación en general, hay trabajo hecho por vendedores como Everett en los años 60 que básicamente observaban aquellas cosas que la gente considera al hacer una elección de adaptación; la adaptación de una innovación.

Entran en juego cosas como ventaja relativa, complejidad y simplicidad de una innovación, compatibilidad, capacidad de prueba y capacidad de observación de una innovación. La capacidad de observación de una innovación es exactamente lo que acaba de mencionar, ¿cómo puede un usuario ver que existe una ventaja al usar esto? Las DNSSEC constituyen una tecnología que vive debajo de la capilla, por lo que tiene todas estas cuestiones que acabo de describir; la ventaja relativa es muy difícil de ver, es muy difícil dar ese mensaje.

Pero está ahí, y estamos hablando de que son todas ventajas a largo plazo. Todo es sobre la seguridad a largo plazo de una infraestructura a nivel mundial. No es directamente algo que active por sí mismo, específicamente del lado del suministro. Es algo con lo que se protege el bien común de Internet y ayudará a innovar.

Lo que hemos estado pensando en conjunto, creo que compartimos esa forma de pensar, es cómo podemos garantizar que la capacidad de prueba, la complejidad y la compatibilidad sean más bajas, que las barreras se vuelvan más bajas. Y eso es haciendo software libre y creando herramientas. Por ejemplo, las herramientas para firmar, que están disponibles en muchos proyectos de código abierto. De hecho, otra parte de esa ventaja relativa es la creación de incentivos.

En los Países Bajos, básicamente hubo un subsidio. Si usted firma sus dominios su tasa de registro disminuye, y es una cantidad pequeña, pero para las empresas de hosting que tienen 100.000 dominios fue una propuesta muy interesante.

De modo que como un registro, a nivel de registro, esos son los cambios que se pueden alentar. ¿Puede usted asegurar que su comunidad de usuarios tienen fácil acceso a las herramientas que se necesitan, y puedes darle un incentivo económico y una ventaja relativa? Pero eso es todo desde una conducción del bien común público. Espero que eso le ofrezca una perspectiva menos tecnológica a su pregunta.

PAUL DONOHOE: Estoy totalmente de acuerdo con el tema de infraestructura, y es por eso que .post ha adoptado una política de 100% DNSSEC, ya que es vital para garantizar las transacciones que van a estar sucediendo en toda la infraestructura. Sólo deseo volver a la cuestión de la capacidad de observación, porque una vez más, es el usuario final quien realmente va a impulsar la adopción, porque ese es el asunto. Tendremos una discusión presencial sobre eso, porque creo que eso es algo muy interesante sobre lo cual deberíamos enfocarnos.

RUSS ARENS: Claro, y también hay... La otra sesión que tenemos, una sesión de todo el día el miércoles, contemplará mucho más de los temas tratados, en mucha mayor profundidad. Uno de los temas importantes que creo que ayudará, en términos de hacer las cosas a nivel del usuario, es la incorporación de la tecnología DANE, que ya hemos mencionado un par

de veces aquí. Podrá escuchar más detalladamente sobre eso el día miércoles, o podemos hablar después.

Pero eso es también algo que moviliza mucho... Una manera de mover la información frente del usuario para que la puedan ver. ¿Más preguntas? Atrás de todo, ¿es una pregunta de la sala de chat? Adelante.

ORADOR: Esta es una pregunta de Carlos Watson. ¿Cuál es el desafío del ISP para promover la adopción de las DNSSEC en el resolutor que gestionan es un problema para resolver, alrededor de un mundo de varios cientos de millones de DNS públicos? Gracias.

RUSS ARENS: En realidad no entendí la pregunta. ¿Tú lo hiciste Roy?

ROY ARENS: ¿Le importaría repetir la pregunta, tal vez expresándola levemente distinto?

ORADOR: ¿Cuál es el desafío del ISP para promover la adopción de las DNSSEC en el resolutor que gestionan es un problema para resolver?

RUSS MUNDY: Si entendí bien la pregunta esta vez, creo que la persona estaba preguntando qué se necesita para obtener que los operadores de

resolutores de todo el mundo pongan en práctica y comiencen a utilizar las DNSSEC. ¿Creo que suena parecido a lo que se preguntó? ¿Si? Bien. Bueno, una de las cosas que constituye un factor importante es que existe una demanda. Todo el mundo en esta sala puede regresar y ver lo que su ISP está haciendo. Ya sea que se trate del trabajo, su ISP de trabajo o de su propio ISP personal.

Si no están ejecutando DNSSEC, y el 8% es una muy buena tasa de adopción a partir de lo que estábamos viendo antes, pero aún deja a un 92% que no cuenta con la compatibilidad. Vayan a preguntarle por ello. Ese es uno de los conductores más grandes que existe, que la gente plantee el tema y lo haga de una manera que ellos entiendan. La demanda es lo mejor que hay si estamos hablando de un tipo de entorno competitivo, como lo son la mayoría de los ISPs. En otros entornos, como de países, sigue habiendo un control gubernamental y aún son fuertemente influenciados por los gobiernos.

Así que aquellos que son capaces de trabajar con los gobiernos que pueden estar implicados en el control de este aspecto, deben trabajar para promover la adopción de los ISPs. ¿Warren?

WARREN KUMARI: Lo ha hecho una cantidad de personas, como *Comcast*, es hacer algo así como un argumento de venta con esto. Hay un pequeño costo para habilitar las DNSSEC en el resolutor de su ISP. Implica un poco de gastos adicionales, un poco de trabajo adicional, pero no es tanto. Lo que se puede hacer es, una vez que lo haya activado, puede decir a sus usuarios el gran trabajo que está haciendo para ayudarles con la seguridad. Usted puede utilizar esto como un elemento bastante bueno de

comercialización o ventas, al transmitir a los usuarios que se preocupan por ellos, que se preocupan por mantener seguras sus interacciones en la web.

De modo que los ISPs pueden utilizar el hecho de que ejecutan DNSSEC como una especie de factor diferenciador. Yo sé que si yo estuviese intentando elegir un ISP, preferiría elegir a alguien que parezca preocuparse por la seguridad y que desee ayudarme a mantener mis cosas bancarias seguras, ante alguien que no lo haga. Creo que usar esto como una táctica de venta es un muy buen truco. Además, una vez que una serie de proveedores de Internet en la región lo hagan, si usted no es uno de los que están haciéndolo y algo le sucede a uno de sus usuarios, ese usuario podría cuestionar legítimamente por qué usted no estaba haciendo todo lo que podía hacer.

¿Estaba usted cumpliendo con su debida diligencia para mantenerlo a salvo? Así que, eventualmente, si usted no está haciéndolo, podría estar exponiéndose a algún riesgo legal en algunas jurisdicciones. ¿No sé si eso era útil de escuchar?

RUSS MUNDY: Excelente, gracias. Sí Joyce, adelante.

JOYCE: Yo sólo deseaba garantizar que entiendo todo. Tal vez usted puede aclarármelo. En cuanto a los actores de DNSSEC, si la zona raíz está firmada y el proveedor del servidor de DNS, la empresa que gestiona el servidor de DNS también está firmada, por lo que todos los dominios

están firmados, entonces, ¿quién más tiene que hacer también su trabajo con el fin de hacer eso?

Por lo que he oído, usted dijo que el ISP... Por ejemplo, en casa estoy usando una compañía de cable para acceder a Internet, ¿cierto? Por lo tanto, ¿son ellos también responsables si quisieran hacer eso, también tienen que hacer las cosas de DNSSEC? Pensé que una vez que los servidores de nombres firmaban, debería ser seguro. Suena como un montón de actores que tienen que esculpir su trabajo.

RUSS MUNDY: Déjeme ver si puedo clarificar esto para usted Joyce. Lo que ha visto antes en la obra teatral fue: la primera parte haciéndolo sin las DNSSEC, realizando la consulta y obteniendo la respuesta. Nuestro Señor ISP, Jacques Latour, era el que iba y hacía todas las preguntas a los distintos servidores de nombres. Después de eso, entonces intervino el Dr. Malvado y tomó la consulta desde el último lugar, pero pudo haberla tomado en cualquier lugar a lo largo del camino.

Ahora, cuando usted firma todo, si no tiene una resolución de validación del servidor de nombres —como el Sr. ISP en nuestra obra de teatro—, el usuario ni siquiera sabe si los datos han sido o no han sido firmados, y mucho menos tiene información para hacer la validación.

Así que hay un papel importante para el resolutor o el operador de ISP —o el usuario final—, de en realidad hacer la validación de las consultas. De modo que primero tiene que ingresar los datos y obtenerlos firmados. En esa parte tiene toda la razón. Pero a menos que la validación de que esa información es correcta sea hecha al momento de

la consulta, usted no obtiene las ventajas de las DNSSEC. ¿Encuentra sentido a esa diferencia?

JOYCE: Sí, pero cuando un dominio es firmado, un DNS es firmado, usted está hablando de APIs y este sitio web está desarrollando la API también, ¿también tienen que...? El API, el programa que quieren, ¿eso también tiene que ser firmado, en forma adicional a que el nombre de dominio sea firmado?

RUSS MUNDY: No, las aplicaciones no tienen que conocer nada acerca de las DNSSEC, siempre y cuando su resolutor de DNS esté haciendo la validación de DNSSEC. Ya sea que el resolutor se encuentre en la máquina del usuario o en su ISP. Las aplicaciones no tienen que... Es mejor si lo hacen, pero no tienen que saber nada acerca de ello. Bien, ¿alguna otra pregunta? Creo que estamos llegando al final de nuestro tiempo. ¿Una pregunta al fondo? Sí, por favor, ¿tiene un micrófono?

CRAIG NESTY: Craig Nesty de Dominica. Noté en su obra de teatro, en el último paso, cuando el secuestro se llevaba a cabo, que el secuestrador no ejecutó las DNSSEC, de modo que básicamente el resolutor capturó eso. Mi pregunta es, ¿qué pasa si hay un servidor de host que no ejecuta las DNSSEC y todos los demás las ejecutan? ¿Son las DNSSEC compatibles hacia atrás con un DNS simplemente normal, o eso rechazaría a ese sitio web por completo?

RUSS MUNDY: El diseño de las DNSSEC da lugar a las cosas que no están firmadas, así como a aquellas que lo están. Si al conseguir las respuestas a la consulta del DNS se llega a un punto en el árbol donde no hay firmas de DNS presentes, eso es claramente identificable dentro del protocolo de DNSSEC y la forma en que la resolución de DNSSEC funciona. Reconocen que no está firmado y simplemente funcionará y la información se resolverá. De modo que no será rechazado si no se supone que esté firmado. ¿Sí?

MIEMBRO DE LA AUDIENCIA: Soy desarrollador de NIC Argentina. Podría hacer una aplicación que detecte la firma en cada paso de la cadena. Haría una aplicación de telefonía celular y deseo hacer... Deseo un programa que me indique si la conexión es con DNSSEC. ¿Podría detectarlas?

RUSS MUNDY: Bueno, existen ahora implementaciones que se ejecutan en telefonía celular. Algunas de las cosas de nuestro kit de herramientas se ejecutan en Android y Maemo —que son OS (Sistemas Operativos) de telefonía celular—, por lo cual ciertamente son muy factibles y si los datos están firmados serán validados. Es una cuestión de examinar cuál es su base de código, cuál es la aplicación que desea utilizar y luego, proceder a la lectura de las especificaciones y escribir el código.

De modo que sí, es muy factible, y nos encantaría ver a más gente haciéndolo. Por favor, vaya para él. Si necesita ayuda para esto, esta es una comunidad increíblemente útil. Nuestro sitio de herramientas

recibe una buena cantidad de tráfico. NLnet Labs recibe una cantidad de preguntas tanto acerca de aquello que desarrolla como acerca de ayuda para la gente que está haciendo más en el mundo de las DNSSEC. Así que por favor continúe. Es alcanzable, no es necesariamente tan fácil, pero si usted se siente familiar con una plataforma y un software, vaya para él.

JULIE HEDLUND: Russ, estamos unos minutos pasados de las 6:30. ¿Podríamos tal vez tomar una pregunta más?

ORADOR: Ha habido un señor detrás de la columna por aquí intentando llamar su atención, si pudiésemos ir por aquí...

MIEMBRO DE LA AUDIENCIA: Mi pregunta es, ¿existe alguna relación entre DNSSEC y SSL (Capa de Conexión Segura)?

RUSS MUNDY: En realidad se trata de dos protocolos independientes. Son complementarios entre sí, si se quiere, en cuanto a que uno trabaja muy bien con el otro. Usted obtendrá una mayor seguridad si utiliza ambos, en términos de su seguridad total, pero están separados aunque se pueden ejecutar al mismo tiempo, en la misma máquina.

Sospecho que algunos de estos chicos sentados aquí lo están haciendo. Mi ordenador portátil no lo hace de modo que no estoy, pero lo hago

todo el tiempo. Es muy bueno. La seguridad múltiple en diferentes capas de protocolo es algo bueno y útil de hacer. ¿Respondió eso a su pregunta, señor?

MIEMBRO DE LA AUDIENCIA: Gracias. Sí, claro.

RUSS MUNDY: Bien. Gracias. Creo que eso es todo. Bien, gracias a todos. Esta ha sido una muy buena sesión y tratamos que cada una de las veces lo sea. Si están presentes en la próxima reunión, ciertamente quedan invitados a venir y a unirse nuevamente. Gracias.

JULIE HEDLUND: Gracias.

[FIN DE LA TRANSCRIPCIÓN]