CR - DNSSEC for Everybody
Monday, March 12, 2012 – 16:00 to 17:30
ICANN - San José, Costa Rica

Julie Hedlund: Gracias a todos por venir. Parece que todavía hay gente que está llegando. Por favor acérquense a la mesa. Creo que vamos a empezar en un par de minutos.

Simon McCalla: Bienvenidos a DNSSEC para todos. Gracias en primer lugar por venir.

El objetivo de esta tarde es un tour bastante breve sobre DNSSEC que está diseñado para darles la posibilidad a aquellos que nunca pensaron en DNSSEC o nunca entendieron o que se preguntaron bueno, no lo entiendo mucho, quisiera aprender un poco más.

Esta es la sesión para eso.

Espero que sea una sesión divertida y para cuando se hayan ido tengan una idea mejor de lo que es DNSSEC, qué significa para ustedes, qué significa para la organización.

Hay una hoja que debería estar sobre la mesa que explica un poco qué es la sesión. Nos dice quien presenta, y atrás hay una lista de recursos bastante simples si necesitan usarlos.

No vamos a parar así que voy a empezar a presentar a nuestros oradores.

Mi nombre es Simón McCalla, soy de ".uk" y estoy muy contento de tener aquí a algunos de los expertos de DNSSSEC del mundo. Y yo por supuesto no soy uno de ellos.

Tenemos a Matt Larsen de VeriSign que es el Vicepresidente de DNSSEC de investigación de VeriSign.

Roy Arends DE NOMINET. Tenemos Russ Mundy que es parte de las personas que ayudan a que las herramientas y la tecnología se implementen en el DNSSEC.

Y tenemos Norm Ritchie de IC que es una de las personas más importantes de los (resolutores) de DNSSEC.

Tenemos expertos aquí así que por favor siéntanse en libertad de hacer preguntas. A medida que vamos avanzando y párenme si hay algo que no entienden.

Vamos a empezar. Muchos de ustedes seguramente piensan que en DNSSEC fue inventado en el ITF hace algunos años y que era algo muy técnico. Pero en realidad eso es una mentira.

El DNSSEC fue inventado hace 7 mil años en el año 5 mil antes de Cristo.

Quisiera presentarles a una señora que se llama Ugwina que es una persona que vive en el borde del Gran Cañón, es muy bonita ella.

Del otro lado del Gran Cañón tiene su novio que se llama Og y el también vive en una caverna que está del otro lado del Gran Cañón.

El problema que tienen ellos dos es que hay un camino muy largo que los separa a ellos dos y no pueden hablar mucho.

Un día ellos se reúnen después de pasar a lo largo del Cañón y se dan cuenta que empieza a salir humo de esa fogata de Og y empiezan a cocinar de algún modo una idea. Y de repente están enviando señales de humo de un lado al otro del Cañón y están chateando divertidos.

Lamentablemente apareció otro hombre que es bastante malo y su nombre es Komansky, y entonces Komansky va pasando y le gusta un poco Ugwina, entonces también va enviando señales de humo y ahora la pobre chica está un poco confundía, no sabe quién está tratando de casarla.

Entonces, se mete en el Gran Cañón para ver cómo resolver este tema.

Cuando llega al otro lado dice “bueno a ver, tengo que empezar a hablar a las personas que están ahí sentadas en el campo”. Y está hablando con una persona que se llama Difi y Difi tiene una idea sobre cómo resolver el problema.

Va corriendo a la cabina de Og y vamos a ver qué pasa.

Y dentro de la cabina de Og hay un color medio raro que es el azul y que tiene arena, es arena azul que está ahí adentro. Va a buscar esa arena y la tira al fuego y entonces está seguro que el humo va a tener ese color azul.

Y ahora Ugwina y Og puede chatear libremente porque saben que cada vez que ese color azul es de Og y cuando (…) es el de Komansky, entonces Komansky está un poco confundido, no sabe qué hacer porque es su plan malvado fue detenido.

Eso es lo que ocurre entonces sobre DNSSEC.

Si hay algo que tienen que recordar es ese humo azul.

Poner algo en las respuestas del DNS es saber qué es lo que va a ocurrir, qué es lo que va a volver.

Eso es todo lo que hay a un alto nivel. Tienen que recordar una sola cosa, y voy a hablar sobre ese humo nuevo. Recuerden ese humo azul.

Ahora, le voy a pasar la palabra a Roy que va a hablar un poco más de lo que es el DNSSEC.

Roy Arends: Les voy a dar una presentación o introducción sobre DNSSEC. Vamos a empezar con conceptos de alto nivel de DNS.

El DNS básicamente es un conjunto y donde ustedes ven un nombre de dominio, cada vez que ven un ".", ese "." Va a separar las etiquetas unas de otras. Por ejemplo, si ustedes toman "….bigbank.com" cada uno de los nombres que están ahí es una etiqueta y todo está básicamente estructurado como un árbol.

Primero tienen la zona de raíz y esa zona de raíz no sabe nada de bigbank.com. Solamente sabe sobre los dominios de primer nivel. Los dominios de primer nivel como ".cr" o ".com" y ".uk", ellos si saben todo sobre el segundo nivel. Como bigbank.com, bigbank.com no sabe nada sobre la raíz y como esto está muy bien separado es muy escalable.

Hay otro sistema involucrado que se llama el resolutor, el resolutor es una pieza un poco complicada porque esta es la máquina que hace todo el trabajo. El resolutor va a empezar con la zona de raíz y la zona de raíz

va a delegar al resolutor al nivel siguiente y así sucesivamente. Esto continúa con una reducción hasta que se resuelven las preguntas.

Esto es increíblemente rápido y hay una enorme cantidad de servidores de DNS y una enorme cantidad de resolutores de DNS. Los resolutores han sido optimizados para ser incluso más rápidos al utilizar un caché, el caché básicamente es donde se guarda la información, se puede imaginar que si entró a ".bigbank" antes no tiene que entrar ahí otra vez porque es poco posible que en un poco período de tiempo la información haya cambiado.

Recuerden esto, a Ugwina, quien cumple el papel de resolutor, está chateando con Og, quien representa al servidor. En nuestro caso Ugwina la resolutora va a chatear con muchos Ogs, algunos Ogs son más feos que otros pero en general así es como funciona.

Voy a presentarles ahora una especie de obra pequeña para mostrarles cómo funciona el DNS. Para eso voy a presentar nuevamente a Simon McCalla, que va a hacer el papel de la zona de raíz, Matt Larsen va a hacer el papel de la zona del ".com". Tenemos a Russ Mundy que va a ser bigbank.com; y tenemos a Norm Ritchie que va a ser el papel de Jose usuario. En esta obra yo voy a hacer el ISP, el proveedor de servicios de internet.

Los usuarios son muy buenos usuarios, el usuario quiere algo, ¿Joe?

Norm Ritchie: Hola voy a ser mi banco así que quiero entrar a www.bigbank .com para hacer mis operaciones bancarias y que mi SP me ayude.

Roy Arends: No tengo idea donde www.bigbank comenta, esto sin efectivo así que voy a empezar en la raíz. Raíz, quiero la respuesta, quiero la respuesta para bigbank.com

Simon McCalla: Gracias ISP la verdad es que no puedo decirte donde está bigbnk.com pero si puedo decir donde está el ".com" está en 1.1.1.1.1.

Gracias.

Roy Arends: Necesito la dirección para www.big.bank.com

Matt Larsen: Bueno, desconozco la dirección para www.bigbank.com . Pero sí puedo decirte que el nombre de servidor de bigbank.com están en están en esa dirección 2.2.2.2.

Roy Arends: Hola bigbank.com. Como 2.2.2.2.2 quiero la respuesta o la dirección a www.bigbank.com

Russ Mundy: Bueno. Yo tengo esa dirección, esa dirección es 2.2.2.3, para www.bigbank.com

Roy Arends: Gracias, ahora tengo esta información y la voy a agregar a mi cache para uso futuro y luego la voy a usar con Jose usuario.

Norm Ritchie: Gracias Sr. ISP, Ahora yo voy a hacer mis operaciones bancarias en 2.2.2.3.

Roy Arends: Esto es en esencia cómo funciona el DNS. Ha estado funcionando así desde hace 30 años, el año que viene el protocolo de DNS va a cumplir 30 años. Y lo que ustedes acaban de ver realmente ocurre en la vida real. Porque cada vez que ustedes escriben un nombre de dominio en el navegador y antes de que vean cualquier cosa esto es increíblemente rápido. Así es como funciona.

Pero es tan antiguo que cuando se diseñó no había seguridad. Entonces estos nombres pueden básicamente ser falsificados y el caché puede ser envenenado fácilmente y la razón es que los DNS utilizan UDP.

TCP es un protocolo de internet que se utiliza de una forma como un apretón de manos. Es cuando uno llama a alguien, uno dice su nombre, el otro le dice el nombre a uno y básicamente le estrecha la mano.

La información que ustedes envían en ida y vuelta tienen como un reconocimiento.

Ahora el UDP es algo distinto porque es como escribir una postal. Uno escribe una postal, escribe un nombre, una dirección, la manda por correo y nunca vuelve a mirar para atrás. Con un poco de suerte en algún punto de tiempo alguien les va a enviar a ustedes otra postal.

El problema es que uno no pueda autenticar simplemente validando la dirección quien es esa persona. Entonces volvemos a la historia del señor de la caverna y ahí (inaudible 41.37) la resolutora, de hecho puede estar muy confundida porque ella no puede decir quién es el verdadero Og.

Les voy a mostrar esto nuevamente en una breve obra y si podemos pedirles a los actores que vuelva, por favor. Esto va a ser muy familiar a lo anterior pero está un poquito cambiado. Muy bien.

Norm Ritchie: Soy JOY USER tengo más facturas que pagar y así que tengo que hacer más operaciones bancarias. Señor ISP yo quisiera ir a www.bigbank.com,

Roy Arends: Gracias, bueno yo ya limpié mi caché pero no tengo ninguna información y solamente sé donde está la raíz. La raíz está en 0.0.0.0. Hola raíz. Quiero que me des la dirección de www.bigbank.com.

Simon McCalla: Hola señor ISP, lamentablemente no sé esa dirección pero sí se la dirección de 1.1.1.1. Esa es la dirección.

Roy Arends: Gracias. ".com" quiero que me des la dirección de www.bigbank.com

Matt Larsen: Bueno no sé específicamente su dirección, pero si puedo decirle que bigbank.com en sus nombre de dominios están en 2.2.2.2

Roy Arends: Gracias, así que ahora ya sé lo que quiere hacer bigbank.com, voy a ir a bigbank.com para que me diga dónde queda www.bigbank.com

Gracias bigbank.com, ahora tengo la dirección para www.bigbank.com y no tengo ninguna forma de decir de dónde viene este bigbank.com

Norm Ritchie: Gracias señor ISP ahora puedo salir y hacer mis operaciones bancarias en 6.6.6.6.

Roy Arends: De nuevo, esto es lo fácil que es falsificar algo. Es tan fácil que va tan rápido como el DNS en sí y la solución para este problema se llama DNSSEC. Es un poco más complicado así que aguántenme un poquito porque voy a tratar de hacerlo mejor.

El DNSSEC utiliza la firma digital para asegurar que la información sea correcta y que venga del lugar adecuado y la criptografía funciona del siguiente modo. Hay dos llaves o claves que están relacionadas unas con otras, una es una llave pública, que es la que le damos a todo el mundo y la otra es la clave privada. La clave privada no se la damos a todos, la mayoría la tenemos para nosotros de una forma muy cerrada. Bien guardado. Porque todo el mundo sabe que cada vez que uno le da esa clave sabe que por ejemplo bigbanck.com está asociada a esa clave y yo

o bigbank.com podemos usar una llave privada para hacer algo y todo el mundo sabe que esa clave privada se puede usar para validarlo.

La criptografía básicamente consiste de varias claves y varias firmas y las llaves públicas y las firmas son parte de la información como en una libreta de direcciones o alguna otra cosa. Lo que ocurre con DNS es que ahora uno puede almacenar estas claves y estas firmas e el DNS. Y se pueden buscar los datos, como uno los busca como uno busca una dirección en un texto.

Hay otro paso que hay que incluir. Para que el resolutor confíe en la zona de raíz tiene que haber una transacción primero. Llamamos a eso "configurar la confianza". Ahora el ancla de confianza es muy conocida y básicamente si uno quiere asegurar el resolutor tiene que configurarlo y por defecto se va a hacer la configuración del DNSSEC.

Pero también, entre "com" y raíz y entre bigbank y ".com" tiene que haber un paso de autenticación también. Entonces en algún punto en el tiempo, las llaves o claves de bigbank, que usa para sus zonas tienen que ser autenticadas por ".com". Y una vez que eso se realiza la zona de ".com", va a ser un registro de DS, y ese registro de DS es una versión simplificada de la llave que bigbank está utilizando.

Bien. Entonces para mostrarles estos, les vamos a mostrar una obra de teatro. Y vamos a la diapositiva. ¿Se acuerdan de Komansky? Ugwina, la resolutora, ahora no puede verificar si el Og real es quien le envía un mensaje, si el servidor de nombres envió ese nombre y el DNSSEC puede usarse para validarlo.

Bien. Eso fue demasiado rápido. Muchas gracias.

Entonces vamos de vuelta al escenario.

Bien. Tomate tu tiempo.

Entonces, el primer paso es. Todas estas zonas necesitan autenticarse una a la otra a sus padres. Entonces COM se necesita autentificar con la raíz. Lo que pasa aquí es un registro de DS implementado en la zona de raíz y ahora podemos confiar a COM implícitamente y lo mismo pasa con bigbank.com y com. Y ya que yo tengo la clave configurada para raíz.com puedo comenzar la validación.

Norm Ritchie: Tengo más cuentas para pagar. Entonces. Señor SP quiero ir a www.bigbanck.com

Roy Arends: Mis caché están vacíos. Vamos a la raíz. Necesito la dirección de www.bigbank.com.

Simon McCalla: Bueno, no sé la dirección pero sé donde está el servicio de nombres y es 1.1.1.1 y le doy el certificado.

Roy Arends: Muchas gracias. Le doy la mano y así confirmo que la información que recibí es correcta. Ahora voy al servidor de nombre ".com". "Dot com" quisiera tener la dirección de www.bigbank.com

Matt Larsen: Ya sabe que no sé, pero si pedo decirle que el servidor de bigbank.com es el 2.2.2.2, así que aquí tiene, le doy la mano.

Roy Arends: Ya puedo validar la información y es correcta. Y ahora voy a bigbank.com

Bigbank.com, quiero tener la dirección de www.bigbank.com

¿Qué pasa? Obtengo la dirección pero me parece que no está bien. Trato de validarla pero no puedo, porque la clave es incorrecta. Trato nuevamente. Quisiera tener la dirección de www.bigbank.com

Russ Mundy: Y la dirección es 2.2.2.3

Norm Ritchie: Y ahora puedo declarar la victoria, ahora tenemos la dirección de www.bigbank.com y (Cruela) ya fue derrotada. Y aquí tiene la dirección de bigbank.com

Muchas gracias señor ISP. Ahora puedo hacer mis cuentas en 2.2.2.3 y muchas gracias por el DNSSEC. Muchas gracias.

Roy Arends: Esto fue una linda obra de teatro. Ahora le paso la palabra a Russ Mundy.

Russ Mundy: Bien. Todavía soy bigbank.2.2.2.2. Bien. Muchas gracias. Nos divertimos haciendo eso y espero que ustedes se lleven con humor algo que es bastante difícil y algo que l agente no sabe y que no están tan conscientes, pero mi porción aquí es para decirles cómo una persona puede implementar el DNSSEC, independientemente de si uno tiene un rango de DNS.

Como ustedes saben hay muchas partes que forman parte del DNS. Son muchos nombres, muchos de ustedes son propietarios de nombres, tienen la titularidad o mentores de un espacio en el DNS, hay mucha actividad para obtener esos nombres dentro del sistema del DNS y manejarlos y gestionarlos y llegar a las personas. Entonces el DNSSEC toca de alguna manera todos estos aspectos. Lo que están haciendo es por ejemplo si ustedes son una actividad de ccTLD las chances son muy altas de que ustedes tengan una confianza en la viabilidad de la función del DNS, ya sea que tengan en la compañía o con un contrato, contratan a una persona que sabe mucho, sobre DNS.

De otra manera si el DNS prolifera en su negocio, pero no está acorde con lo que ustedes dicen, ustedes pueden tener todas las actividades de DNS tercierizadas en alguien más. Por lo tanto quisiera describir este conjunto de cosas que están involucradas o que podrían estarlo.

Tal y como un operador de ccTLD u otro tipo de operador que sea muy importante, que sepa temas de DNS. Muchas compañías como HP o IBM tienen personal que sabe mucho de DNS y si ustedes son una empresa que está tan crítica ustedes pueden registrar su nombre con este servicio y lo pueden contratar.

Y aquí vemos una ilustración del árbol del DNS y ustedes pueden ver que está estructurado como un árbol, acá está la empresa HP, por ejemplo, acá hay otra empresa CNN por ejemplo, CNN es una página muy activa, muy grande, pero el negocio central son las noticias, así que pueden o no tener mucho personal de DNS.

Pueden o no. Pero si ustedes tienen personal que sabe mucho de DNS y saben mucho de las funciones de DNS ustedes tal vez querrán hacer las actividades de DNSSEC con la misma estructura que ustedes tienen de personal. Si ustedes lo terciarizan en otra actividad, ustedes lo van a hacer también de esta manera para las piezas de DNSSEC.

¿Dónde están todas estas piezas? Aquí vemos algo que hice hace unos años para una reunión de ICANN, para ilustrar que el contenido de DNS es la parte importante. Cuando hicimos nuestra obrita, la dirección de IP del usuario JOE para que no sea falsificado, hizo algunos pasos para evitar la falsificación, pero ellos son los registradores o propietarios y esto está a la izquierda como lo ven.

Tenemos los registradores que pueden estar o no presentes en cada una de las zonas, pero son muy comunes por zonas muchos tienen los registradores. Y los registros todos los TLD tienen un registro, todos los TLDs tienen que tener un registro para que funcione.

Después son las operaciones de servidores de nombres. Y cada zona tiene que tener una operación de servidor de nombres esto es un servidor existente, pero la gente piensa automáticamente en algunos caos donde los registradores tienen que ser los operadores de servidores de nombres.

No necesita ser el caso, esto puede pasar pero no necesariamente.

Tiene alguien que operar la maquinaria de nombres.

Tenemos en la otra parte los resolutores, y las aplicaciones para usuarios finales. Hay muchas partes involucradas y esta es la dirección del contenido. Hacia arriba y después hacia abajo ala derecha.

Acá tenemos una ilustración de los componentes del DNS. Acá tenemos www.bigbank.com, por ejemplo, alguien tiene que poner esta información en el servidor de nombre autorizado y después el cliente hace la pregunta aquí, el usuario Joe quiere tener, sale las respuestas y el usuario Joe obtiene la respuesta y si tenemos una empresa muy grande, aquí vimos una ilustración. Matt Larsen la hizo para una versión de CNN.com y nos muestra la constelación de nombres, entonces la dirección puede ir a cada uno de ellos.

Y aquí vemos una ilustración con una herramienta que mi personal desarrolló para mapear dónde están las respuesta de DNS y esta página web ya la hicimos hace cuatro años y son las preguntas que se necesitan para llenar una página. No solamente una pregunta o dos. Si tenemos una página muy grande hay muchas preguntas y esto continúa creciendo. Esto pasó hace seis meses. Aquí tenemos las (…) de DNS. Esto pasó esencialmente en un abrir y cerrar de ojos. ¿Cuánto lleva cada vez que uno va a www.cnn.com para que se llene la página?

Es bastante rápido y todas estas (…) pueden pasar en el momento, antes de que la página web o a medida que se llene la página web. Entonces, lo importante que yo quiero decir en esta parte de la página son los

datos, los nombres, la información de direcciones de IP. Esto es lo importante.

De eso se trata el DNS y cuando uno se lleva la seguridad de DNS a cada una de las piezas, cualquiera sean las piezas, una cosa importante para recordar es que son los datos del DNS que son los más importantes. El DNSSEC fue creado para proteger esos datos. Y como ustedes vieron en la obrita que hicimos alguien puede meterse y sustituir los datos de ustedes. Pero de todas maneras son los datos de DNS los que protege el DNSSEC. Y muchas veces se hace mucho énfasis en la protección de materiales gráficos de DNSSEC en detrimento de la protección de los datos de DNS en sí.

Aquí como les mostré anteriormente, todas las piezas a la izquierda de la pantalla son los sitios donde los datos se vuelcan a un DNS y a la derecha podemos ver el funcionamiento del cableado del DNS. Esto es lo que protege el DNSSEC. Pero aún a la izquierda hay cosas que se necesitan hacer con el DNSSEC.

Como ustedes vieron y si ustedes se acuerdan del estrechamiento de manos es darle confianza hacia arriba del árbol. Y eso tiene que ocurrir antes que el mecanismo obtenga y saque los datos del árbol.

El flujo es como explicamos el DNSSEC, es en la maquinaria de funcionamiento del DNS.

Como ya les dije anteriormente, cuando ustedes encuentran su lugar dentro de la estructura de DNS piensen qué es lo que están haciendo. Y les voy a dar unos ejemplos en un minuto. Ustedes probablemente van a usar el mismo enfoque que están usando hoy. Tienen personal que sabe

mucho, ustedes tienen un contratista que lo hace por ustedes. Entonces si ustedes están operando una operación muy grande de DNS hoy en día, probablemente van a querer usar los productos existentes que ustedes están usando en la actualidad e incorporar el uso de DNSSEC.

Por ejemplo, comprar un producto como ven acá en pantalla, la semana pasada tuve una reunión con Microsoft y tienen mucho progreso, vieron Windows 8, en esa línea de productos hay muchos avances y otros productos de código abierto que están disponibles ahí.

Y hay otra actividad que está muy (entuciasmante), al menos a mí me entusiasma mucho porque soy un (…) de DNS.

Esos son los servidores de firma. Lo que hacen ustedes en las operaciones de DNS si por alguna razón no es posible incorporar un cambio ya sea en los registros o en servidor de nombre o en la estructura de la empresa, existen los servidores de firma a los que ustedes le dan las firmas, se las envía a VeriSign o Nominet o a cualquier otro y ellos hacen la firma de los datos por ustedes y les envían los datos a ustedes. Entonces ustedes obtienen un archivo más grande, pero ustedes no tienen que hacer ningún cambo a su maquinaria más allá que tomar el flujo de los datos que van a su servidor de nombres.

Enviarlo a esta empresa y cuando vuelve, vuelve al servidor de nombres.

Como dice la diapositiva, lo que hagan ustedes en una instancia en particular puede ser una mezcla de todo lo dicho anteriormente.

Entonces, si ustedes están utilizando un producto, y no voy a mencionar ningún producto específico porque hay muchos, tenemos una encuesta

de productos de DNSSEC pero hay muchos productos que no tienen ningún seguimiento de DNSSEC.

Por eso si ustedes tienen algunos de estos productos y van al proveedor y le dicen “lo vendes a DNSSEC?” No bueno, no puedo.

Ahí hay una elección para hacer. Utilizar productos diferentes, lograr que el proveedor los consiga. No es que uno va y pide un producto y el proveedor dice “bueno, todavía no lo tenemos”. Pero lo que yo sugiero es que vayan y lo pidan porque por lo menos dentro de algunos años – hace algunos años lo que hemos escuchado del DNS es que los clientes están pidiendo, entonces, por favor pídanle al proveedor que les de lo que ustedes quieren y sé que hay varios de ustedes que ya lo hacen pero, hay otros que todavía no.

También es posible que dado el entorno, de nuevo el servicio de firma podría caer en una instancia, pero es mucho más fácil que encaje que cuando uno tiene el control total de la operación.

Si ustedes son los propietarios de un nombre, yo tengo varios nombres registrados. La mayoría de ellos están relacionados con el trabajo, otros son personales, yo ni siquiera sé cuál es el total de nombres registrados, pero yo sé que hay otra gente que las empresas tienen cientos de nombres.

Tienen ustedes que examinar qué es lo que están haciendo con la gestión de los nombres que ustedes registraron y pensar cómo hacer que esos nombre se incorporen en el DNS como zonas firmadas por los servidores autorizados.

Por eso si ustedes están usando un registrador y están brindando un nombre, le preguntan cuándo pueden empezar a ofrecer el servicio de operaciones de nombres de servicio firmadas.

Y entonces compran un servicio adicional. Si ustedes están operando su propio nombre de servicios –servicio de nombre – ahí empieza a aparecer el problema que mencionamos antes.

Entonces es una situación similar pero ustedes tienen que considerar qué es lo que van a hacer en el mundo general de las cosas. Para llegar al punto efectivamente, en que los datos firmados están en la zona y tienen DNSSEC y que el resolutor validador esté bien, la información que se necesita para validar a su usuario final. Ese es el final de la presentación. Algunos de los enfoques de más alto nivel de lo que ustedes deben hacer. Pero aquí va a retomar SIMON con algunas de las preguntas y le voy a pasar la palabra a SIMON.

Simon McCalla: Gracias Russ. Primero una pregunta a la sala. ¿Les resultó útil lo que vieron hasta ahora? ¿Les pareció útil? ¿Aprendieron algo nuevo?

¿Hay algo que deberíamos haber cubierto y no lo hicimos?

Julie Hedlund: Por favor si se pueden acercar a la mesa donde hay micrófonos y cualquiera que quiera hablar por favor usen los micrófonos porque estamos grabando la sesión y nos va a ayudar a todos a escuchar mejor.

Pedro (…) Hola. Gracias. Mi nombre es Pedro. Soy local y quisiera saber un poco más sobre el DNSSEC.

¿Está definido en el ITF en las revisiones? ¿Hay alguna versión relacionada con esto, es un protocolo? ¿Está actualmente a nivel de redacción o está estandarizado?

Gracias.

Simon McCalla: Roy ¿quieres responder esa pregunta?

Roy Arends: Mi nombre es Roy Arends. Matt y yo, Matt está aquí en la mesa, hemos trabajo en la estandarización del DNSSEC.

Básicamente esta versión del DNSSEC.

Entonces el DNSSEC es un estándar y lo es de acuerdo con el IETF que propone estándares, varios son propuestos. Eso básicamente quiere decir que está bastante bien implementado. Hay documentos escritos sobre las mejores prácticas y si ustedes las quieren buscar los nombres son 4033, 34 y 35. Pueden venir a hablarnos a mí y a Matt.

Simon McCalla: ¿Alguna pregunta aquí al fondo?

Participante: La autenticación entre el servidor de dominio de alto nivel y el servidor subyacente se hace como lo vimos. Pero mi pregunta es ¿Quién autentica el servidor de raíz en sí?

Hay un pedido que viene del resolutor hacia la raíz y no hay ninguna autenticación de ese nivel.

Pero después de eso hay una autenticación del servidor de raíz –

Participante 2: En DNSSEC no hay un concepto de autenticación de servidor sino un concepto de autenticación de datos.

Participante 1: Entonces, ahora, hay una consulta que viene de los usuarios y que se envía al servidor de raíz.

Para asegurar que ese pedido llega al servidor de raíz si y que contiene los datos que van a la capa subyacente.

Roy Arends: Bueno. No hay ninguna garantía que cuando uno envía una pregunta termine en el servidor adecuado. No hay garantía de eso. No hay ninguna seguridad de que cuando se envía una consulta termine en el servidor correcto. Pero en última instancia se recibe una respuesta que contiene una información que luego se puede autenticar, entonces en teoría no importa de dónde proviene la información porque se puede verificar si es correcta o no.

Hay autenticación de datos si independientemente de donde viene, en general viene de la zona de raíz, o de la zona “com” etc. Pero a fin de cuentas uno tiene que estar seguro de que tengan la información correcta o no. Independientemente de donde proviene.

Participante 1: Gracias.

Simon McCalla: Cuántos de ustedes que están aquí están involucrados en la implementación del DNSSEC o pensaron en la organización del DNSSEC en su organización. ¿No hay nadie en esa situación?

Muy bien. Poca gente. Y en qué etapa están en esa implementación del DNS? ¿Ya lo hicieron, lo están pensando? Dígannos, cuéntennos.

Participante 1: Nosotros hemos tercerizado la mayoría de nuestro DNS de los dominios que tenemos registrados. Tenemos algunos parámetros que no tienen DNSSEC y tenemos que mandar nuestros dominios a otros registradores.

También llevamos adelante nuestros propios nombres de dominio y ¿en qué etapa están de esos recursos disponibles?

Bueno estamos bastante bien.

Posiblemente estamos a nivel de nuestros clientes.

Estamos dándoles también a ellos estos datos.

¿Y el resto de ustedes en qué etapa están de esa línea de DNSSEC?

De la implementación del DNSSEC?

Lito Ibarra: Soy Lito Ibarra del Salvador. Estamos pensando en eso y ahora quisiera preguntar. Alguien mencionó esta posibilidad de enviar una zona para que sea firmada por otro y luego que vuelva. Yo quisiera preguntar en cuanto a esa posibilidad cuánto tiempo se demora en minutos y hasta qué punto es seguro.

Simon McCalla: ¿Matt podrías hablar de la zona de VerySign?

Matt Larsen: Depende del servidor, pero en general es bastante rápido. Tarda minutos o quizás segundos. Y en general se utiliza un protocolo llamado T-Sager. Hay algo compartido en secreto entre ustedes y los servicios firmados, por eso ellos saben que tienen las zonas de ustedes y ustedes saben que reciben la zona adecuada también.

Simon McCalla: Hay una cantidad de zonas firmadas, algunas los hacen gratis, otros cobran, entonces, hay algunas organizaciones que también tienen que ofrecer un servicio de firma. Entonces se está convirtiendo en una parte importante de que particularmente si no tienen los recursos para implementar el DNSSEC en sí, los servicios son un muy buen paso.

En algunos sentidos es una piedra inicial para que podamos seguir avanzando con el DNSSEC y otras personas están pensando en implementarlo.

Es algo que podemos hacer todo el tiempo.

¿Alguien más que esté pensando en el DNSSEC?

¿Tienen que decidir si lo tienen que implementar o no?

Louis Pulan: Hola. Soy Louis (Pulan) de ".qt" y estamos haciendo la reingeniería de todos nuestros software, desde hace 10 años hemos tenido el mismo software que era prácticamente manual. Y si estamos pensando en incluir DNSSEC. Pero ahora es sólo un proceso de pensamiento.

Simon McCalla: ¿Está pensándolo por usted mismo o quiere un servicio de firma o cómo lo está tomando?

Louis Pulan: Estuvimos considerando ambas cosas. Necesitamos –estamos en la Universidad, necesitamos mano de obra gratis, pero no estoy seguro de que lo podamos hacer con ellos. Y por eso estamos buscando otras posibilidades.

Simon McCalla: ¡Excelente!

Participante: Una sugerencia sobre el proceso de reingeniería. Tengan cuidado con los productos para saber si son de código abierto o son comerciales para poder asegurar que soportan la base RFC que tiene el DNSSEC. Porque incluso con el servicio de firma, ustedes van a tener que correr los servidores de nombre que van a tener que estar respaldado por las RFC.

Eso es algo que tiene que ser una piedra fundamental para entrar en quien sea que esté operando y que tiene que cumplir con la funcionalidad de los nombres del servidor.

Louis Pulan: Excelente sugerencia.

Simon McCalla: ¿Alguien aquí tiene alguna preocupación sobre el DNSSEC? ¿Alguien piensa que no es una buena idea? Hay muchos que piensan en DNSSEC y otros que piensan que no es una buena idea. ¿Hay alguien que piense eso o que esté preocupado? Bueno, lo voy a tomar como un "no".

Quisiera hacer una pregunta rápida a nuestros panelistas. Si hubiera una o dos tips que ustedes quisieran dar o están pensando en la implementación del DNSSEC. ¿Cuál sería?

Roy Arends: Yo estuve involucrado en muchas etapas de la implementación del DNSSEC y si quisiéramos implementar actualmente el DNSSEC no tendríamos que pensarlo demasiado. Hay muchos software que puede gestionar el DNSSEC, por ejemplo hay un OPEN DNSSEC que lo mencionó Mandy y básicamente hay que hacer un poco de ingeniería pero hay una

gran cantidad de información en cuanto al tamaño de las claves, en cuanto la firma frecuente o no frecuente.

Básicamente hagan lo que hace la raíz y van a estar en una zona segura. Usen los últimos términos de referencia, los últimos DNS para poder darle servicio a la raíz, para poder también gestionar la clave, y van a estar en una zona segura.

Simon McCalla: Gracias.

Matt Larsen: Bien. Quisiera agregar también que hay muchos recursos para ayudarlos. Tenemos una lista acá. En la lista que les dimos tenemos mucha información sobre DNSSEC, cómo funciona, su despliegue y su implementación.

Muchas personas les van a poder ayudar con los recursos con los que se cuentan. También las iniciativas de DNSSEC que les mencionó Russ. Otra es los análisis de operaciones. Hay muchos lugares donde ustedes pueden hacer preguntas específicas sobre DNSSEC.

Simon McCalla: Muchas gracias Russ. ¿Qué tenés para comentar?

Russ Mundy: Quisiera seguir lo que dijo – las sugerencias que ya se hicieron no reinventen la rueda, busquen la información que esté disponible, que está allí, que se aplica a la situación de ustedes. Muchas de las personas

con las que tuvimos interacción a lo largo del tiempo. Usen mucha energía para crear cosas que ya existen en realidad. Entonces, por favor usen los recursos que están disponibles. Hay muchas personas que están ahí que con gusto les van a responder las preguntas y hagan los pasos poquito a poquito no traten de completamente tirar el sistema de DNS simplemente porque están haciendo DNSSEC.

Si lo van a remplazar al sistema DNS no lo remplacen del todo, pero no hagan una restructuración importante simplemente porque tienen que hacer el DNSSEC. Si se justifica si, háganlo, eso si no háganlo paso a paso, poco a poco.

Simon McCalla: Norm, ¿Quisieras hablar sobre el DNSSEC?

Norm Ritchie: Quisiera también reiterar lo que dijeron otros. No es que se quiera innovar. Hay muchas personas que ya lo están haciendo. Hay muchas personas inteligentes que están ahí, entonces no tienen que reinventar nada. Hay muchas personas que se dedican a eso y que con mucho gusto les van a ayudar a solucionar los problemas.

Las referencias de DNS están aquí, hay productos que cumplen con los requisitos de DNSSEC, la última versión 9.9 que ya está disponible para el mercado.

Roy Arends: Quisiera agregar una cosa más. Desde los días tempranos hay mucha información y dudas sobre si se agrega seguridad.

Si agrega seguridad y no hay problema con el DNSSEC. La raíz está firmada “com” está firmado, “uk” está firmado, no hay ninguna razón por la cual no hacerlo. Todas las razones son para hacerlo. Muchas gracias Ross. ¿Alguien acá tiene alguna otra pregunta que quisiéramos cubrir? ¿Hay algo en lo que los podamos ayudar?

Muchas gracias.

Luis: Soy Luis de Costa Rica. ¿Como el DNSSEC trata las claves de firma y replicación? Cuándo hay una expiración y ¿cómo se trata esto en el sistema de DNS?

Roy Arends: El DNSSEC es diferente del TLS o sistema de certificados. DNSSEC no hay un mecanismo de replicación más allá del tiempo. Por ejemplo el registro de DNS se firma el que tiene una hora que está válida de X a Y. Entonces la etiqueta de tiempo tiene que ser más corta. No tiene que ser todo el minuto, pero no tan corta ni tan larga. El cache elimina la información una vez que se vence. Esto tarda uno o dos días.

Simon McCalla: El punto es que si hay un compromiso o un problema con la clave, vamos a otra nueva clave con implementación y se propaga en todo el DNS. No tiene que ir y venir. Eso no tendría ningún sentido.

Bien. Si no hay mayores preguntas, tenemos todo un día sobre información de DNSSEC que va a ser el miércoles, creo que comienza a las 8.00.

Julie Hedlund: Es el miércoles 18.30 en la sala La Paz C arriba y vamos a tener una actualización regional. Hay personas que están implementando el DNSSEC, hay ejemplos del mundo real. Hay básicamente muchísima información. Los invitamos a que participen y también va a haber un almuerzo al final.

Que esto es una yapa. Muchas gracias por venir. Muchas gracias por tener la oportunidad de hablar sobre el DNSSEC.

Simon McCalla: Quisiera darles las gracias a los muchachos que me ayudaron con esta presentación y vamos a estar acá disponibles si ustedes quieren hacer alguna pregunta.

Muchísimas gracias por haber participado.

Fin de la transcripción -