COPENHAGUE – Taller sobre las DNSSEC -- Parte 2
Miércoles, 15 de marzo de 2017 – 11:00 a 12:45 CET
ICANN58 | Copenhague, Dinamarca

DAN YORK: (…) estadounidense Comcast. Y Paul [incomprensible] está aquí para contarnos qué están haciendo en Comcast. Paul, tienes la palabra. Les cuento a los participantes remotos que este es un debate. Por eso no tenemos tantas diapositivas, así que por favor aprovecha la oportunidad de hacer preguntas por el chat, que está siendo monitoreado por si tienen preguntas porque hay gente que está participando remotamente.

Cuéntanos, Paul, qué está haciendo Comcast para prepararse.

PAUL: Tenemos dos infraestructuras que soportamos. Una que soporta 26 millones de clientes en el lado del cliente, y también el lado corporativo en IT DNS. Hacemos validación para ambos grupos. Por tal motivo, cuando se produzca el trasvase, tendremos más de 300 servidores recursivos en el lado público y 50 o 60 en el lado interno. Hemos decidido que aun cuando estamos usando otras máquinas vamos a tratarlos a todas como BM, por una

cuestión de seguridad, configuradas para el tipo resolutor que tenemos.

El anterior no era un método válido porque configuraba la validación en nuestras verificaciones. Entonces estamos validando la clave en el laboratorio, verificándola y haciendo la automatización. A partir de ahí avanzamos. En el laboratorio entonces lo manipulamos. Creo que ese es el plan. La mayoría de las empresas que usan AWS, qué ejecutan los resolutores en máquinas virtuales están haciendo algo así.

DAN YORK: Entonces básicamente pulsamos el botón y ahí está. Es una estrategia bastante sencilla. Matt, ¿lo has capturado para la próxima presentación sobre la KSK?

PAUL: No lo podía hacer básicamente en un único punto de diapositiva porque no lo puse pero porque no está operacional todavía. ¿Alguien tiene alguna pregunta para Comcast sobre su estrategia para el traspaso? Bueno, muy sencillo.

Ahora tenemos a [Tobin] de [incomprensible].

[TOBIN]: Espero que puedan comprender mi inglés hoy. Me levanté a las 4 de la mañana. Estoy un poco cansado además.

Me llamo [Tobin] [incomprensible] y me siento intimidado aquí sentado junto a Comcast. Soy cofundador y operador de la compañía Interland. Quizás han leído en los cálculos que tenemos para Suecia. En esa área verde pequeñita ahí es donde yo vivo. Son 50 municipios los que firmaron los dominios y cada uno de estos municipios tiene su servidor DNS. Soy responsable de un grupo muy pequeño de 30.000 abonados. Diez ISP pequeñas. Soy responsable de los resolutores de DNS y vamos a basarnos en la RF6 50-11. Tiene 2 resolutores nada más, un maestro y esclavo. Espero que funcione.

Cuando me invitaron a esta conferencia, decidí utilizar el sistema [incomprensible]. Espero que esto funcione.

Pero también configuramos varios resolutores y validación para nivel empresarial. No sé cuántos, pero también [incomprensible] cómo resolutor de desempeño y facilidad para fines de facilitar el sistema. Bueno, este es mi caso, mi estrategia para el traspaso de la llave. Y espero que funcione.

Creo que hay una página más. Sí. Algunos problemas. Quizás escucharon hablar del incidente de hace 10 años de [incomprensible]. Yo fui el que firmó el dominio. Eso lo pueden leer después. Es del DNS, no es algo de validación. Antes de

firmarse la raíz, teníamos problemas de KSK. Pero desde entonces no hemos tenido problemas.

A veces he oído decir que la gente le pregunta el tamaño de la clave. Tenemos algunos municipios que tienen más de 10 claves y las podemos manejar correctamente. O sea, que a mí no me preocupa. Bueno, eso es todo.

Casi.

DAN YORK: Fíjense en la remera que está usando Tobin. ¿Alguna pregunta?

MENA: Gracias. Entonces para [incomprensible]. Cada versión desde el 2011 va a resolver su problema con el traspaso de la clave, así que creo que en los últimos 6 años instalaron una versión anterior. Ahora estarán en una situación sin problemas para los municipios. Con 50-11, con [incomprensible] o una alternativa. Hay un procedimiento alternativo para descargar la nueva ancla de confianza de ICANN.

TOBIN: Algunos de los resolutores funcionaron igualmente, debo decir.

DAN YORK: ¿Alguna pregunta? ¿No? Bueno, estamos avanzando rápido aquí. Me parece que este panel no era tan necesario, lo cual no está mal. Ahora vamos a hacer las cosas más complejas y le voy a pedir a Andre que nos cuente su experiencia en el mercado de los ISP.

ANDRE: Muchas gracias. El ISP nunca se concentra en el DNS. Es un servicio de transporte al cual no le prestamos demasiada atención. Entonces es como una norma de la institución ahora involucrarse un poco más. Dije antes que desarrollamos un widget que comprueba si los resolutores soportan DNSSEC. No tengo forma de decir si el resolutor está bien configurado para soportar 50-11. Sería fantástico añadir esta funcionalidad con un widget, pero esto sin un registro firmado no lo podemos lograr. Ese es el problema.

Por eso intentamos comunicar lo más posible nuestras acciones con la comunidad de ISP porque se firmó antes de firmar la zona raíz. Los primeros ISP pusieron el check, como una marca de confianza. Entonces luego pasaron a la cadena de anclas de confianza y también tenemos contactos directos con ellos. Hablamos directamente con ellos, tenemos conferencias, hablamos de los temas y también tenemos buenas relaciones con los puntos de intercambio de internet locales, lo cual genera

el grupo de operadores de red. A los ISP les damos las novedades de lo que está pasando en el DNS a través de estos ámbitos.

Creo que si los resolutores que tienen instalados son los adecuados nada va a pasar. Son distintas las soluciones de algunos. Con ellos hablamos especialmente con cuidado, que comprueben que la solución que adquirieron esté bien. Creo que va a ser un paso de éxito. No tengo miedo del 11 de octubre.

DAN YORK: Gracias. No veo preocupación. Están todos tranquilos con el 11 de octubre. Matt, me parece que no es necesario que sigas haciendo las presentaciones. Está todo bien. Bueno, a ver qué puede decir Erwin.

ERWIN: Yo también. ¿Qué puede pasar de malo? ¿Qué hay de difícil? Voy a decir algo parecido a lo que dijo Andre. Los ISP que yo conozco tienen buena gente especializada en redes, que saben lo que hacen. Probablemente tengan soporte de software para 50-11, que permite comprobar el 11 de octubre. En el Grupo Corporativo estará Matt, que se asegurará de que la gente haga lo que dice que va a hacer. Hay otra acción de difusión qué son los proyectos de software. [Incompresible] es un nuevo espacio

que para los ISP. También [Incompresible] tenemos que asegurarnos que esté integrado en los paquetes de software, los Linux, los [Incompresible] y otros proyectos. Tenemos que asegurarnos de que actualicen los paquetes y también los sistemas operativos que incluyan validación. Tenemos que encontrar la forma de incorporarlo con tiempo a través de notificaciones o lo que fuere. Con esto digo que estoy tranquilo, pero tenemos un par de áreas que no estoy seguro. Los black boxes. Las empresas que tienen black boxes y que hacen validación y que ellos no saben porque es una caja negra que hace DNS y un día deja de funcionar porque lo dejaron en el sótano y no vino ningún consultor a explicarle y nadie sabe qué hacer. Este es un área que a mí me preocupa, que la gente no sepa que existe DNSSEC.

DAN YORK: Paul, ¿quieres hacer un comentario?

PAUL: En los Estados Unidos el mayor problema .gov compraron mucho DNS basados en artefactos, en equipo, y considerando los problemas presupuestarios se perdió apoyo. En lo que hace a las anclas de confianza, .gov está muy por encima de todo lo demás que nosotros estamos haciendo.

DAN YORK: ¿Algún otro comentario? bien. Roland, cuéntenos qué están haciendo.

ROLAND: No voy a hablar sobre lo que estoy haciendo, sino sobre lo que quiero hacer en realidad.

La próxima. Las acciones del operador entran en una sola diapositiva. Vamos a hacer un-bounding. Esto incluye la nueva etiqueta del ancla de confianza en el un-bound en el día K. lo llamo día K porque 11 de julio es el día importante, que será la primera vez que tendremos la clave. El día k comenzaremos a monitorear este archivo y comprobaré que los repositorios en los resolutores tengan la ingeniería correcta para que entren actividad. Espero que el software lo manejan solos. Solo estaremos para comprobar que estén los espacios de lectura en el unbound. Operadores en nuestra unidad constitutiva están trabajando a través de distintas medidas de mitigación con las universidades. Algunos nos envían el tráfico, otros hacen su propio tráfico. Le tenemos que decir a esta gente que presta atención. También tenemos algunos usuarios de equipos en nuestra unidad constitutiva, gente que hace sistemas [incomprensible] para hacer resolución de DNS. Bueno, va a ser interesante ver si estos negocios positivos toma la clave.

Lo que quiero contarles es una idea que ya he hablado con algunos, por ejemplo Roy [incomprensible] de la ICANN, que es medir el traspaso de la clave. Estuve buscando fotografías. Encontré está del canario en la mina de carbón. ¿Quién conoce esta expresión del canario en la mina de carbón? bueno, no todos. En la época en que se hacía minería del carbón no había energía limpia. Los mineros solían llevar un canario en la jaulita a la mina. ¿Por qué? El canario es muy sensible a los gases en el medio ambiente. Sí el canario empezaba comportarse de manera extraña o se moría, era una señal de que había que evacuar la mina porque estaba pasando algo malo.

Me gustaría ver que pudiéramos implementar algo parecido para el traspaso. Me gustaría poner un canario en la mina de carbón virtual con el propósito de rastrear el impacto operativo del traspaso y que actuará como una advertencia temprana, como una señal de que los resolutores de validación no están validando la clave nueva. Tengo un motivo ulterior porque como yo vengo de la comunidad académica quisiera escribir un bonito paper sobre esto. Entonces quiero recabar datos de medición de validación del traspaso desde la perspectiva global para aprender de este tipo de acontecimientos.

La idea es utilizar cuatro perspectivas. Usar las ondas [incomprensible], hacer algo que se llama [incomprensible]. ¿Quién trato de mirar Netflix y quiso ver los contenidos

estadounidenses y se los bloquearon? Levanten la mano. Todos miramos Netflix. Hay empresas que proveen servicios VPN entre pares. Entonces la máquina actúa como nodo de salida de conexión VPN. En la Universidad de [incomprensible] de los Estados Unidos mediremos esto, que es muy bueno porque tenemos visibilidad de las redes residenciales, lo que ATLAS hace pero no da visibilidad de las redes residenciales de los expertos en la red. Entonces quiero usar su metodología para hacer medición de validación en estos nodos. Ellos tienen casi presencia global. Hay muchísima redes residenciales, que es un punto de partida muy interesante. Igualmente quiero seducir a la gente de APNIC, que sigue haciendo estas mediciones tan interesantes como para que incluyan esta medición también en sus mediciones. Probablemente lo que están haciendo lo podemos aprovechar. O sea, trabajar a partir de lo que ellos ya recopilan. Por supuesto también analizar el tráfico a los servidores de nombre raíz. Sé que hay gente que planea hacer esto para evaluar cómo se afecta al traspaso de la clave.

Quería establecer un nivel basal de validación antes de KSK. Queríamos tener una señal y la relación de ruido. Vamos a tener intermitencia, algunos van a validar, otros no. Y queremos saber antes de que comience la nueva clave. Mi idea básica este momento es hacer esta medición de forma diaria o quizás aumentar luego la frecuencia si es factible y/o deseable. Cuanto

más nos acercamos al 11 de octubre, más deseable sería por lo menos en alguno de los proveedores residenciales. En ese caso quizás sería bueno subir la frecuencia. Esperamos poder tomar alguna medida. Si el canario empieza a cantar o si se muere significa que hay un operador que va a estar teniendo problemas con un resolutor. Y nosotros como comunidad podemos contactarnos con ellos y decirles: "esto es algo serio tienen que hacer algo ahora. Tienen que resolver esto".

Muchos de nosotros tenemos contactos en la comunidad de los operadores y si podemos de alguna forma hacer que esto sea un esfuerzo de la comunidad vamos a poder asegurarnos de que esto no se convierta en un desastre sino que se convierta en el éxito que todos pensamos que va a ser. La próxima por favor.

Mi plan es comenzar en la cuarta semana de abril. Quiero comenzar a evaluar qué clase de datos queremos recopilar y como quedamos recopilarlos. Me encantaría recibir el aporte de ustedes. Ya registre root canary punto org. Todavía no pude hacer nada más, pero como dijo Matt, esperamos tener un sitio web muy bien diseñado y muy atractivo. No es entonces un sitio DNSSEC. Root canary punto org no tiene la firma DNSSEC. A propósito, no está firmado con DNSSEC.

A propósito... Y creo que sea mi última diapositiva. Sí. Es la última. Si tienen alguna pregunta, sugerencia, háganlo. Pueden

hacer comentarios o enviar emails. Dan, seguramente haya algunas preguntas pero yo tengo mi propia pregunta. El servicio [incomprensible], ¿se puede usar de manera gratuita?

ROLAND: Sí. El servicio se llama [incomprensible]. Están esas cosas que nunca lee cuando dice "sí, acepto". Eso les da los derechos para usar su Usuario.

DAN YORK: Increíble. Yo no uso ese servicio pero es bueno saberlo. ¿Hay alguna pregunta? Warren y después Roy.

WARREN: ¿Podría retroceder dos diapositivas por favor? El DNSSEC de APNIC, Jeff Houston y George piensa en trabajar en estos cuando se haga el traspaso principal de la clave. Ellos les van a dar datos a la ICANN.

ROLAND: Sí, sí. Me dijeron.

WARREN: En general les llevo un día hacerlo. Van a tratar de hacerlo más rápidamente esta vez. Creo que los servidores de la raíz también

van a hacer este ejercicio en determinados momentos. ¿Podemos ir una diapositiva adelante?

ROLAND: Quisiera que nos expliques por qué queremos hacer esto desde múltiples perspectivas. Porque si miramos solamente APNIC, vamos a tener cierta visibilidad. Pero el problema con la medición en APNIC es que no podemos reproducir las mediciones en los mismos lugares de manera confiable. Dependemos de la red. Entonces nos da visibilidad pero no reproducibilidad. [Incomprensible] nos permite elegir la salida. Entonces nos permite hacer que sea más reproducible, pero cuesta muchísimo más. Es mucho más caro que la medición de APNIC. Entonces estamos tratando que distintos proveedores lleguen al mejor nivel posible.

WARREN: La próxima diapositiva. Por lo que vi el modo de falla probable es simplemente que la validación se detiene completamente. Si uno está haciendo validación significa que toda la resolución de DNS se detiene completamente. Entonces los operadores se supone que se van a dar cuenta de eso. ¿No es cierto?

¿Hacemos ahora preguntas generales también? Esta es una pregunta general también. Es decir, para gente como Comcast

se supone que ustedes tienen una población por detrás que eres envía consultas y que hace validaciones. ¿Saben cuál es esa población? Porque aun cuando quizás ustedes estén trabajando, si ellos están validando van a llamar. Hay distintas razones por las cuales va a pasar esto: Gente que hace ejecutar su servidor de nombres y que no tiene un sitio de archivos persistentes o que no leen es archivo. O quizás Dan, Julie, Steve han estado haciendo también el trabajo de DNSSEC para principiantes, que la gente sol vida y hay dispositivos, etc. Entonces aquellos que utilizan resolutores de validación o cualquier tipo de resolutor, ¿tiene algún plan para ver qué porcentaje de usuarios vale están haciendo la validación?

Además ¿hablaron con la gente que tiene que tener un código de escritura listo, para si hay un problema así es como tienen que hacer la detección de problemas del DNSSEC por ejemplo?

ORADOR DESCONOCIDO: No tenemos una buena forma de saber qué pasa en la cadena resolutoria. Lamentablemente casi todo hoy en día tiene algo predeterminado. Entonces esto hace que las cosas sean un poco más complejas. Tenemos una idea bastante buena de lo que pasa con los resolutores dentro de nuestra empresa. De hecho, hacemos cosas nuevas como n-map, scans y muchas otras cosas. Para estar atentos a esto, el grupo más grande que

todavía no empezado a utilizar el [incomprensible] normal tiene lo mismo que nosotros: Automatización. Entonces una vez que nosotros les decimos que pongan el ancla de confianza [incomprensible] o lo que sea, se ocupa de eso.

La población que a mí me preocupa, los ISP se quejan de CPE y las actualizaciones. Podemos trabajar con DNSSEC. Incorporamos el código. Ahora si buscan fondos a través de [incomprensible] podemos hablar después.

Nosotros no tenemos forma de controlar el archivo config, que lo activa. Lo que sabemos es que la mayoría de la gente que tiene CPE, los únicos que lo activaron son aquellos cuyo código nosotros controlamos y lo hicieron de forma deliberada y Aquellos cuyas actualizaciones tenemos nosotros también. Entonces tengo que coordinar con la gente que es dueña del XP3 y los otros dispositivos del CPE. Todavía no empezamos a hablar con la gente de primera línea. Este va a ser un desafío interesante.

DNSSEC en general ha sido levemente problemático. De pronto, parece que es DNS y cae en mi grupo, y nosotros lo resolvemos, lo enfrentamos. Ese es el punto en el que estamos.

ORADOR DESCONOCIDO: ¿y el firmware? Hay una indicación que dice hagan clic en este botón y va a tener DNSSEC, así que hay otras cosas que se están haciendo.

ORADOR DESCONOCIDO: Sí, lo entiendo, pero nosotros no tenemos la visibilidad o la forma de hacerlo. En algún momento lo que va a pasar y lo que pasa con otros CPE es que uno elige el propio y en teoría va a quedar conectado para que ese proveedor brinde soporte. Va a ser difícil que los proveedores hagan las actualizaciones, como dije, ISP, CPE, etc.

DAN YORK: Roland, ¿quiere responder?

ROLAND: Sí. Dos comentarios. Warren dijo que los operadores muy grandes los afilia seguramente solo es que van a hacer esto. Lo que nosotros vimos con los problemas de validación con algunos de estos TLD, en dónde tienen glitches, se publicaron las claves equivocadas el algoritmo falló y todo lo que estaba por debajo del TLD falló, y todo lo que estaba por debajo del TLD desapareció. Supongo que lo que está diciendo es que si esto pasa nada y todo lo que estaba por debajo de la raíz vas a desaparecer.

Pensamos que esto puede ser así. Veo la señal negativa con la cabeza, pero hay otras dos cosas que podrían ocasionar problemas porque en algún momento durante el traspaso de la clave habrá un momento en donde el DNSSEC va a ser muy grande. Eso no significa necesariamente que en la resolución se vaya a detener completamente todo el tiempo. Y el otro problema es que todas esas distribuciones de Linux por default, si es simplemente la última versión estarán los resolutores que van a funcionar correctamente. Yo hice algunas mediciones en los servidores autorizados para ver dónde está el crecimiento en términos de validación de DNSSEC y hay una gran cantidad de resolutores que solamente trabajan con una pequeña población de clientes, pero la cantidad de resolutores está aumentando muy rápidamente. Esa gente también hay que monitorearla.

DAN YORK: [Ron], [Bennie], Roy.

ROY: Muchas gracias. Creo que esta es una idea fantástica. Me refiero a la idea del canario. Me parece que es fantástica. Yo empecé a proponerla hace unas semanas por primera vez. Inmediatamente todos en nuestro equipo en la ICANN lo apoyamos de manera entusiasta. Tenemos nuestros propios datos, los datos de la raíz L que recopilamos. También

analizamos eso. Nos gustaría realmente ver este aspecto del estudio. Esto no es casual. [Incomprensible] es muy bueno, pero son 2 días. Esto para todo el período del traspaso de KSK. Así que sí, tienen todo nuestro apoyo.

DAN YORK: [Incomprensible]

ORADOR DESCONOCIDO: No es una pregunta en realidad, sino que estoy repitiendo una pregunta que se le hizo al panel de traspaso de KSK ayer. ¿Qué pasa si la actualización automatizada no funciona? ¿Debería haber (y es una pregunta para los operadores y una pregunta también general) una publicación o información acerca de cómo hacer la reparación manual o habrá un lugar en donde se va a publicar esta información, dónde se les va notificar a los operadores que tienen que tomar alguna medida? ¿Debería haber un lugar al que todos puedan dirigirse si tienen un problema con los resolutores, con la preparación, con [incomprensible], cosas que no funcionan, puede probar esto, esto o lo otro, o quizás el sitio web de los resolutores? es una pregunta. No es una sugerencia. No quiero generar trabajo para otros. Es una pregunta para los miembros del panel.

ORADOR DESCONOCIDO: Yo creo que es una buena idea. Es lógico. Si la gente puede contactarse con un sitio, en caso de que falla la validación, pero eso es otra cuestión. Y como dijo Paul correctamente, probablemente tengan que hacer eso con los dominios que no están firmados.

Yo creo que es una buena idea hacerlo. Y también podría ser un proyecto de la comunidad. La gente que produce paquetes de código abierto podría decir: "estos son cuatro pasos simples para reparar el resolutor".

ORADOR DESCONOCIDO: No puedo hablar en nombre de Matt. Matt, ¿volvió? Sé que la gente de la ICANN hablaba sobre las cosas de [incomprensible], hacer que las cosas estuvieran disponibles en algún lugar, en tutoriales, y asegurarse de que todo funcionara. Y ahora yendo a su punto quizás tendremos que pensar en la posibilidad de asegurarnos de que esto esté disponible para los dominios no firmados. Buen punto. Ahí está Paul.

PAUL: Me preguntó un poco en broma: Hay una dirección de IP que todo el mundo conoce, en la que uno podría utilizar un sitio web y podría utilizar cuando el DNS falle. Entonces, Warren, ¿por qué

no escribe una página con información en ADD? Para los que no lo saben Warren es de Google qué ópera eso. Y acá esta Mike.

MIKE: El riesgo de entrar en la solución del problema en este momento es que si tenemos un ancla de confianza mala en el resolutor no vamos a resolver nada, ni siquiera dominios firmados. Entonces no es una cuestión de poner algo, sino que tiene que ser algo que está bien. No sabemos dónde poner la señal de advertencia. Lo pensamos pero no sabemos dónde ponerlo.

DAN YORK: La señal de advertencia de Internet.

ORADOR DESCONOCIDO: Ni siquiera va a reparar o resolver el problema de los resolutores.

DAN YORK: Buen punto. Vamos a seguir pensando en esto. Roland.

ROLAND: Quiero agregar algo más. Si usted desconfiguraron las búsquedas y si bloquean algo que no tiene un ingreso DNS reverso no van a poder loguearse a esa máquina.

DAN YORK: Fantástico. Ahora Oliver y después [incomprensible].

OLIVER: Gracias. Con respecto a lo que dijo Roland, la falla va a traspasar así que esperamos que la gente vaya buscando estas fallas. Uno puede operar 1,2 o 3 resolutores. Creo que Paul opera algunos más que eso. Entonces si hay algo que está mal va a afectar a una pequeña población y en muchos casos los clientes finales van a tratar nuevamente y es de esperar que puedan pasar a otra caja. Pero creo que su idea acerca de monitorear y hacerlo desde una perspectiva global es una idea muy buena. Quiero apoyarla. Así que sugiero que se cree una lista de mailing por invitación para aquellos que están dispuestos a hablar con ustedes sobre este tema. Hay cierta información que puede compartirse, pero hay otra información que no puede compartirse.

Con respecto al otro punto, tenemos este canal de comunicación fantástico cuando pasan cosas malas, que se llama Twitter. Entonces ¿por qué no creamos un hashtag notificación sobre el traspaso de KSK? No digo que debamos llamarlo falla, sino notificación, para que todos puedan hacer un seguimiento.

DAN YORK: Podemos hablar con los spammers sobre esto. El día K. ¿Podíamos al 11 de julio llamarlo día K? ¿Podía ser ese el nombre oficial? ¿Alguna otra pregunta? [Incomprensible]

ORADOR DESCONOCIDO: Tengo una pregunta para Roland. El root canary punto org pareciera ser muy importante para los operadores, así que quisiera introducir este sitio web a los operadores locales. Quisiera presentárselo. Ahora ¿será posible? Porque si los operadores piensan que pasó algo, van a conectarse con los operadores de la raíz y será una especie de ataque DDOS, así que me preocupa mucho eso. La información es importante, pero ¿cómo podemos distribuirla?

ORADOR DESCONOCIDO: Veamos si alguien me puede ayudar para hacer magia y que esto no ocurra.

DAN YORK: Hay algunas personas que podrían tener acceso a CDN. Quizás podrían ayudarlo y participar.

WARREN: Uno de los temas importantes en muchos documentos como SSAC 63 y 73 es que debería haber mucho trabajo de difusión

externa para contactarnos con aquellos que normalmente no participan. Creo que uno de los temas es que hemos tenido demasiado éxito con el impulso del DNSSEC. Si quiere activar DNSSEC tiene que implementar SSAC 63, que es fantástico. Hagámoslo ahora. DNSSEC para todo ese tipo de cosas. Lo que me asusta es la cantidad de personas que activaron esto porque nosotros sugerimos que era lo que había que hacer y después se alejaron o se fueron de la empresa o se fueron a otra parte y hay muchas cajas no administradas o no gestionadas. Y no va haber nadie ahí que sepa qué es, cómo activarlo o cómo desactivarlo.

Alguien dijo que ISC tiene un sitio web que informa acerca de DNSSEC. Lamentablemente cuando las cosas salen mal la gente no se preocupa por reparar la clave. Simplemente desactiva la validación porque es lo más fácil y lo más rápido. Y una vez que hicieron eso desapareció el dolor y la gente se va.

DAN YORK: Sospecho que tiene razón.

ORADOR DESCONOCIDO: Mi experiencia con las fallas de validación es que en la mayoría de los casos no es el traspaso de la clave sino que sacan las firmas porque no saben que tienen una zona firmada y casi de

forma universal cuando explicábamos lo que tienen que hacer para resolverlo desactivan DNSSEC.

DAN YORK: Peter [incomprensible].

PETER: Yo sugiero que podemos hacer una limpieza de primavera del DNS sec. Cuando la gente pone las manos en la configuración de resolutor para automatizar el traspaso automatizado o para instalar la nueva clave, yo voy a instalar la nueva clave. ¿No es cierto? No solamente vamos a destruir algo, sino que esa es una buena oportunidad de hacer dos cosas correctas al mismo tiempo.

ORADOR DESCONOCIDO: Y desactivar DLV.

DAN YORK: ¿Cuántos de ustedes cambiaron la configuración del resolutor en algún momento los últimos 6 meses? No es la sala correcta para hacer esta pregunta. Otra pregunta. Si consideráramos toda la población fuera de esta sala en ICANN, ¿cuántas personas promedio han cambiado o han visto la configuración de DNSSEC en el último año? Exacto.

ORADOR DESCONOCIDO: Me parece que hemos sobrecomplicado el tema. Quizás podemos retrasar la pregunta porque cuando no tenemos un plazo la gente vive obviamente con las manos metidas en la configuración. Estamos actualizando el software a través de defaults, como para que la gente no se dé cuenta. Dumb down a nivel de usuario podría ser útil.

DAN YORK: CPE es algo real. Cuando la gente compra este equipo en Estados Unidos, consiguen el router porque es mucho de lo que hacen los ISP en los Estados Unidos: Alentar a la gente a poner el router, excepto que hay que actualizarlo. Hay problemas de configuración.

ORADOR DESCONOCIDO: Conozco la situación de Red Hat. Me pregunto, porque recién hablé con una de las escuelas politécnicas que querían hacer DNSSEC. Ellos usaban un servidor autorizado como secundario y tenían muchas firmas copiadas. Yo nunca lo había visto antes es un bug del Windows Server del 2012. No habían desplegado la cadena de dependencias para instalar este fix. Entonces me pregunto si esto generaría problemas de validación también. Creo que si uno es un usuario de Windows legítimo, Microsoft

probablemente sepa que fix es uno ha desplegado y cuáles no porque tiene que ver con la licencia. Me preguntó si esto se aplica también a otras grandes plataformas de software, como Umbtu o Red Hat. Si tienen visibilidad de cuánta gente por lo menos descargo los paquetes como para saber que se están comportando bien.

ORADOR DESCONOCIDO: La persona de pie detrás del micrófono quizá sea la que pueda responder.

PAUL: Tenemos algunas estadísticas, pero como hay mucha gente que corre clúster detrás de los servidores proxy, no sabemos exactamente cuántos están actualizados. No obstante, en nuestras soluciones es más sencillo. No ha habido paquetes desde hace más de un año porque quienes encuentran bugs en el software de Red Hat requieren un nuevo software. Entonces la política estándar de Red Hat es que Red Hat es muy estable y no queremos cambiar. Si usted quiere cambiar algo por favor presente un informe de bug indique que necesita un soporte DNS porque en tanto no haya clientes que soliciten no hay tracción. Entonces presente un informe de bugs si tiene una licencia genuina, así nosotros podemos pasar a nuevas versiones.

DAN YORK: ¿Alguna otra pregunta para los panelistas? vamos. Los que están detrás. ¿Algún ISP? adelante.

ORADOR DESCONOCIDO: Un comentario para que la gente de ICANN siga. Me preocupa el tamaño de las claves. No es más problemático que cualquier otra cosa, pero quien ha hecho validación ha encontrado paquetes grandes, sabe que es un problema. Después de los fallos de la zona del DNSSEC, el gran problema no es propiamente el del DNSSEC sino el tamaño de los paquetes grandes. Es algo que tendremos que observar de cerca.

ORADOR DESCONOCIDO: Si compramos CPE y encontramos un proveedor de confianza, en mi caso funciono. Si algo no funciona bien, sé dónde encontrarlo a mi proveedor. Warren habló de los informes de SSAC. Hay algunos que son excelentes.

BERT: Estoy de acuerdo. Quiero agregar un comentario breve. En [incompresible] podemos ver qué versión corre la gente del software, lo cual nos permitiría advertir más selectivamente los despliegues importantes, que es algo que vamos a hacer en

especial porque no estamos implementando el 5011, así que es importante que lo hagamos bien.

Otro comentario. Como Paul, yo soy un representante de la comunidad de operadores porque yo hablo con las firmas que tienen grandes resolutores acerca de cómo los manejan. La situación es bastante deprimente. Me hueco del sentimiento de la gente que apagó, desactivo validación a la primera señal de problema y que puede ser que lo vuelva a activar. Mi sugerencia sería no solo decirles a todos lo extremadamente importante que es porque estaremos condenados si no lo hacemos bien antes, sino también proporcionar materiales listos para aquellos que no nos escucharon. Decirles: mire, a esta página tiene que ir, estas son instrucciones de cortar y pegar para que el sistema no se caiga, sino que funcione bien.

Mi sugerencia para finalizar es que los proveedores grandes de Europa no tienen gente trabajando en los resolutores porque siempre tienen otras cosas que hacer.

DAN YORK: Quiero agradecerte, Bert, por el trabajo que has estado haciendo con el DNS, con el DNSSEC, estadísticas y demás. Así que un especial agradecimiento.

BERT: De nada.

DAN YORK: ¿Alguna reacción?

ORADOR DESCONOCIDO: Por curiosidad, ¿qué partes del RFC 5011 ustedes odian más que no la van a implementar?

BERT: Power DNS. Son 7 personas con opiniones muy firmes a las cuales yo les voy a transmitir su preocupación porque yo no sé cuáles son los motivos, pero pasare la pregunta.

ORADOR DESCONOCIDO: Un documento que creo debemos producir es el que se acaba de describir. Alguien que esté específicamente focalizado en los operadores con materiales de presentación que estarán disponibles desde hoy hasta el traspaso, pero necesitamos mejorarlo porque está en formato de diapositivas ahora. Va a estar pronto en nuestra página web y luego les daré la URL para descargarlo.

ORADOR DESCONOCIDO: Colectivamente hablamos de cómo hacer un sitio simple, algún micrositio para gente como la comunidad de operadores raíz puede saber. Por ejemplo, si DNSSEC se cae tiene que hacer esto o aquello. No necesariamente tiene que estar en el sitio web de ICANN.

DAN YORK: Yo pensaba en el sitio de ustedes y el nuestro. A veces son URL muy complicadas que quedan enterradas. Creo que colectivamente tendríamos que pensar en cómo simplificarlo.

¿Alguna otra pregunta comentario? En la encuesta que ustedes están haciendo, Ron, del día K, quiero hablar porque en el informe del 2017 es en verano ¿no? Porque estará publicado para la ICANN 60. Así que hablemos para ver cómo podemos tener por lo menos información preliminar porque sería interesante.

Si no tenemos más para el panel de ISP vamos a darles un aplauso a todos los panelistas. Entonces ahora pasaremos a una demostración. Vamos a ser usados y valientes. Paul [incomprensible] nos va a acompañar. No hemos reconocido que [incomprensible] aquí presente es el hombre de las estadísticas de los distintos sitios. Usted lo mencionó, pero DNSSEC y IPv6 Es su responsabilidad. Él es el hombre que escribe sobre la cabra de IPv6 que se quemó en Suecia. Todos

queríamos conocer. Búsquenlo y encontrarán esta historia de la cabra de la IPv6. Es la cabra de Navidad. Busca en la en comparación con la cabra de Pascua o la cabra de otoño. No sé. Es algo que existe en Suecia, que se quema todos los años y que esto proporciona estadísticas. No soy yo, sino que son ellos.

ORADOR DESCONOCIDO: La última Navidad duro como 2 horas antes de consumirse.

DAN YORK: ¿Y por qué los suecos queman cabras? No se me ocurre por qué, pero son las cosas que pasan ahí. Pero también hay estadísticas interesantes sobre IPv6 y DNSSEC, incluidos condados en Tejas. ¿No era eso? ¿O donde en Estados Unidos?

ORADOR DESCONOCIDO: Sí, 2 en Tejas pero hay otros sitios. Ahora hay una nueva versión y no tuve tiempo de arreglarlo.

DAN YORK: A mí me pareció entretenido. La manera de defender IPv6 en Suecia era través de los condados de Tejas.

Ahora estamos en el momento de la presentación en que veremos líneas de comando en la pantalla, lo cual es

complicado. Entonces vamos a ver si Paul puede hacer IPSEC oportunista usando DNSSEC si podemos con una demostración.

PAUL: Me parece que la exigencia es mucha. Yo soy parte del proyecto [incomprensible], que comenzó hace un tiempo. Lo comenzó John Gilmmer del EFF con la intención de encriptar la Internet cada vez que pasaba un paquete usando IPSEC. Todavía no llegamos ahí pero seguimos trabajando. El motivo por el cual se armó el equipo era que quería poner claves públicas en el DNS, como para tomar las claves con seguridad y usarlas para hacer conexiones seguras las máquinas. O sea, planeaban usar DNS como una base de datos de seguridad distribuida jerárquica.

Primero, algunas diapositivas para explicar. Una VPN típica cuando la gente piensa en una VPN. Esta es una VPN de sitio a sitio. Hay dos servidores que conectan dos redes u oficinas que se conectan y las comunicaciones fuera de las nubes no están encriptadas. Están al aire libre y los servidores VPN que conectan estas dos redes están encriptados y son seguros. No es la situación ideal pero es una configuración común.

Vemos cada vez un impulso mayor para encriptar todos los componentes individuales de esta red. Obviamente nos gustaría usar IPSEC para eso. Esta es otra configuración de VPN. Recuerden el extremo remoto, el hogar o la oficina. Teníamos el

dispositivo en roaming que se conecta en un servidor VPN, que se conecta desde VPN a la nube. Este es el modelo que usan Netflix por ejemplo. La gente en Estados Unidos desde la laptop se conecta a la VPN que no está encriptado, pero en el servidor después está abierto.

¿Qué es IPSEC oportunista? Necesitábamos algunas funcionalidades que no teníamos hace 15 años. Con IP2, qué es el protocolo de intercambio que se usa para IPSEC para negociar las claves en el túnel, no teníamos una autenticación asimétrica, donde el cliente fuera anónimo. Este es el modelo de TLS. En un sistema seguro hay que asegurarse de identificar el servidor. Pero el servidor no tiene deseo de identificarlo a usted. No es anónimo. Con la IP2 pudimos hacer este modelo.

Una de las razones por las cuales hace una adecuada esto no funcionaba es porque IPSEC tenía que tener una clave propia. La laptop tenía que poner credenciales y eso requería publicarla residenciales y era un problema más difícil de resolver. Otra cosa que necesitábamos para el despliegue era DNSSEC en el host local.

Olvidé decir antes que hay cada vez más resolutores que se están usando. Esto está bien porque la gente corre resolutores en las laptop y en los teléfonos. Entonces tienen DNSSEC hasta el nodo de extremo de la máquina. Entonces no está la última

milla insegura en la máquina. Eso es importante. Y eso nos permite hacer triggering basado en DNSSEC. Cuando enviamos un paquete a un destino remoto o a un host remoto y sabemos el nombre, podemos buscar la clave de IPSEC, instalarla y armar el túnel y se corre la aplicación.

Otro problema es que teníamos que resolver el problema de NAT. IPSEC utiliza el túnel en el dispositivo y la única IP que se tiene no permitía esto. Tuvimos que encontrar una manera de conectar múltiples personas al mismo servidor sin causar conflicto. Elaboramos una buena idea. Redactamos un borrador que venció pero lo vamos a hacer y el código. Todo esto es invisible en el nodo de servicio del subsistema. O sea que evita conflicto. Así es como funciona el flujo del paquete. Tenemos una aplicación como Firefox que hace una búsqueda en el DNS para buscar por ejemplo [incomprensible] punto org. Puede ser unbound o [incomprensible] el servidor local. El servidor local entonces lo que hace es validar el registro A, hacer la resolución, pero en paralelo envía una consulta para el registro IPSEC key. Y solo cuando tiene una respuesta de ambas consultas continúa diciendo entonces en el siguiente paso del proceso. Si hay una IPSEC key, primero envía el [incomprensible], más el registro A, más la IPSEC key, más el [incomprensible]. Eso se encripta. Recién entonces el servidor DNS retorna al registro A la aplicación. De modo tal que cuando la aplicación recibe o

resuelve el registro tiene la dirección IP y envía la información no encriptada, pero que está en lo que es el IPSEC.

Esto es importante. Lo llamamos encriptado oportunista porque el usuario no lo ve. Lo tratamos de ocultar lo más posible para que sea seguro y si no podemos hacer la autenticación hasta la última milla, aun así previene la interferencia. Esto no es un reemplazo de la barra de dirección verde o cualquier otra indicación de que está autenticado.

Habiendo dicho esto, trate de hacer un diagrama para qué lo vean al hacer la demo. Lamentablemente mi pantalla es un poco más chica de lo que pensaba. De modo que hay una superposición de muchos de los términos que puse con mucho cuidado. Voy a poner aquí la máquina en medio, y luego aquí está Peter [incomprensible]. Podemos ir viendo lo que ocurre. Si voy al primer servidor, todo está desactivado ahora. Esto es para tener un nivel basal. Si ejecuto un PIN. ¡Qué interesante! ¡Qué rápido! Ahí está. Ahí vemos el PIN. Leemos el texto. No está encriptado. Esto es rápido. Nos aseguramos de que empecé de limpio. Vemos si hay algún túnel. No hay. Todavía no lo integramos en la superficie del DNS. Lo estamos haciendo y nos vendría bien ayuda. Por ahora es un módulo independiente. Este concepto estaría dentro del servidor DNS.

Funciona mejor si escribo IPSEC. Ahí está. Voy a volver porque pasé muy rápidamente. Entonces primero hemos que tener el registro A. Tenemos el registro A protegido por DNSSEC. Encontramos el registro IPSEC key. Tenemos acá los datos crudos para aquellos que implementan DNSSEC, que ya hicieron alguna implementación de registros IPSEC key, les pido disculpas pero si le sirve de algo yo hice esto a la 1:00, así que este es el peor registro diseñado por el IETF. Si decodifican esto correctamente, van a obtener esto, que es el IPSEC key. Entonces lo sacamos de acá, hay una interfaz para llevar esta clave al servidor de IPSEC. Veamos si entra en una pantalla. Ahí estamos.

Básicamente el equivalente a esta conexión dice acá. El lado izquierdo que es el lado del cliente utiliza autenticación nula. Es decir que no se auténtica porque es la laptop. El derecho encontró la dirección IP y la puso en conexión. Y el resto básicamente son términos IPSEC internos muy interesantes para el mundo del DNS. Después carga la conexión, la inicia y acá vemos algunos parámetros, las claves de acuerdos, establece el túnel. Vamos a ejecutar el pin de nuevo. Vemos que todo está encriptado. Básicamente estamos enviando muchos túneles de IPS basándonos en datos de DNSSEC y esperamos poder acelerar esto para que esto ocurra de manera predeterminada. ¿Alguna pregunta?

DAN YORK: ¿En serio? ¿Eso fue todo? ¿No hay preguntas?

ORADOR DESCONOCIDO: Solo habló de registros A. Entonces va a ser A y cuádruple A porque si vuelven seis registros A tenemos dos opciones. Podemos tratar de hacer 6 túneles, o si no podemos, digamos que tenemos uno de los registros A que puede ir en el túnel, tenemos que decidir le voy a mentir a la aplicación y solamente le voy a devolver el un registro A o ¿qué voy a hacer? Esas son algunas preguntas interesantes cuya respuesta venimos posponiendo.

DAN YORK: Esa era una pregunta dirigida a usted, el partidario del IPv6 local. Veo acá un par de personas que quieren hacer preguntas.

ORADOR DESCONOCIDO: Ayer me encontré con firewall que hacía la intersección, así que tuve que pasar al firewall que yo controlaba. El punto es como vamos a hacer sobrevivir a todo lo de la próxima generación. El usuario va a ver una luz verde pero no a estar verde.

ORADOR DESCONOCIDO: A propósito no les estamos dando el a los usuarios el feedback porque pensamos que esto está por debajo del nivel del estamos tratando de subir la encriptación a Internet sin darle al usuario un sitio web específico autenticado con una luz verde o una barra verde.

Si no está de acuerdo con esa funcionalidad y prefiere texto, siempre solamente texto, entonces también podemos hacer eso. Esto se puede llevar a la aplicación. Hay gente que lo hizo con distintas adopciones y después se pudo usar el feedback pero de forma inherente van a llegar a la pregunta de qué pasa si no funciona, si se hace una falla dura o blanda, como hablamos con el usuario. Decidimos no ir por ese camino todavía. Creo que al principio solamente tenemos que poner la encriptación por default en general y si quieren hacer algo autenticado en el sitio web, un pago bancario, en ese caso no están tan seguros de que dé la aplicación hacia abajo, dependientemente del transporte que esté encriptado correctamente.

PHIL: Supongo que no recibieron muchas preguntas porque todo el mundo está pensando por qué hace 25 años que no tenemos esto. No, es una broma. Pero ahora es posible hacer esto, así que fantástico. Y creo que alguna de las preguntas que surgieron

quizás tiene que ver con lo que yo voy a preguntar ahora. ¿Se puede usar el DNS para una política específica? Es algo que me que me haya perdido algo y se haya dicho ya.

ORADOR DESCONOCIDO: Una de las fallas de este proyecto fue que permitía que se usaran gateways y usaran un DNS reverso y con DNSSEC implementado esto es diferente. Podemos decir que todo el tráfico de este barra 24 va a esta dirección IP, pero en realidad depende de tener un árbol reverso seguro. Por lo que vemos, este árbol reverso nunca fue accesible a los usuarios e incluso cada vez pasa menos. La mitad de las veces mis árboles reversos desaparecen, así que me parece que reverso ya no es una fuente estable. Por eso queríamos alejarnos de eso. Entonces cuando se me ocurrió la idea de interceptarlo a nivel de DNS, el problema fue que solo tenemos el árbol hacia delante y no al reverso. Si no tenemos soberanía sobre la dirección IP, entonces no puedo encontrar ninguna afirmación con respecto a las direcciones IP, quién es el dueño que les escribe claves públicas. Y quizás una vez que tengamos PKI y todos esos proyectos avancen, quizás hay alguna interfaz del usuario final para que puedan usar eso. En ese caso el vamos a poder considerar, pero yo me he mantenido alejado del PKI porque yo tuve suficientes problemas con la gente de DNS y no quiero que toda la gente de enrutamiento también me ataque.

ORADOR DESCONOCIDO: Sí, sería interesante saber cómo van a iniciar la sesión.

ORADOR DESCONOCIDO: Actualmente tenemos distintos modos de falla. Si no se encuentra una clave en DNS, entonces ahí permitimos el tráfico de texto, plain text. Pero hay ciertos grupos, grupos que podemos marcar, y esto es más bien un caso de uso en la nube, dónde se hace autenticación por certificados o mutuamente certificados por registros del DNSSEC. Uno quiere garantizar que todo eso está encriptado porque lo que nosotros controlamos no puede fallar. Entonces decimos solamente el tráfico encriptado puede pasar a este lado. 10/8 solamente encriptado y después podemos hacer excepciones. Tener algún servicio que esté autorizado. Nosotros tenemos clientes que dijeron que por cuestiones legales necesitan que haya cierto tráfico que pueda hacerlo. Este problema con el que nos encontramos es que cuando empezamos a implementar esto en las redes internas, hay muchos firewalls que se tornan inútiles porque ya no podemos ver más nada. Una de las preguntas de uno de nuestros clientes fue se puede exponer el número de puerto de alguna forma al hacer el encriptado para ver qué es. Y nosotros lo convencimos después de un tiempo de que si hacían eso, eso significa que cualquier atacante también lo va a poder hacer y el

firewall va a ser inútil. Entonces lo mejor es pasar a firewall en el nodo final y distribuirlo con algún mecanismo.

ORADOR DESCONOCIDO: Gracias. ¿Y cuándo vamos a tener esto en RedHat? Era una broma.

ORADOR DESCONOCIDO: Primero pasa por Fedora hasta RedHat. Pero yo de hecho envío un paquete para la regla 7.4 también anoche a la una de la mañana. Y eso ya tiene la capacidad de encriptado oportunista para certificados. Si usted puede poner eso en su nube interna y tiene un CA y certificados en el host puede tener esta oportunista. Es decir, cualquier host en la nube para poder conectarse con otro host que esté en su nube.

DAN YORK: Paul seguramente sugirió que si quieren esto el Red Hat tiene que presentar un ticket de incidente.

ORADOR DESCONOCIDO: No. No hace falta. Esto fue para un cliente importante. No hay problema.

DAN YORK: Estaba tratando de ayudarte. Más bugs para software del DNS. IPCSEC está bien.

¿Carson? ¿Alguien más tiene alguna pregunta para Paul? Quiero agradecerle a Paul por haber hecho una demo en vivo.

Tal como acabo de decir por Twitter, probablemente somos el único lugar en toda la conferencia que tiene líneas de comando en pantalla. Es fantástico. Pasando de las líneas de comando a las líneas de gráfico, tenemos acá un voluntario que va a hablar sobre ECDSA. Te voy a dar la palabra a Roland, quién va hablar sobre este tema.

ROLAND: Sí, falta la primera diapositiva, pero la idea. Gracias. Esta presentación es sobre la adopción de ECDSA en DNSSEC. Un punto de vista sobre tres gTLD, un TLD especial, muy especial, y siete ccTLD. Es un trabajo que hice como investigador y como empleado de [incomprensible]. Supongo que todos sabrán que ECDSA fue estandarizado para DNSSEC en 2012, pero nadie lo utilizo hasta que yo fui a una reunión de la ICANN y dije: "nosotros vamos a hacer DNSSEC con ECDSA". Y no se utilizó en absoluto hasta fines de 2015. Les voy a cantar un poco más acerca de lo que hicimos. Teníamos menos de 50 dominios en nuestro conjunto de datos con ECDSA. Después en 2015 Cloud Flair anunció el DNSSEC universal. Tenemos el inicio de DNSSEC

universal, DNSSEC sobre la marcha y después en 2016 el algoritmo predeterminado.

¿Significa esto que la gente lo empieza a usar y podemos ver esto en nuestro conjunto de datos? Un breve resumen. ¿Por qué usar ECDSA? Si es que uno no lo está usando, ¿por qué debería pasar a usarlo? DNSSEC sufre de problemas de alcance debido la fragmentación. Antes Paul habló sobre esto. Y sí, sigue siendo un tema en 2017 y no va a desaparecer, me temo.

Y después el segundo problema es que se abusa de DNSSEC para ataques de amplificación. Se usa de manera indebida, ya sea por protocolos vulnerables, que se usan de manera indebida o lo que fuera, pero hay muchos informes acerca de que los principales ataques de amplificación utilizaban este tipo de dominios. Y la causa común es que DNSSEC tiene mensajes grandes debido a las firmas y a las claves RSA, y la solución es utilizar criptografía de curva elíptica porque hay más claves, hay firmas más chicas y seguridad criptográfica mayor. Entonces básicamente tenemos todo lo bueno en un algoritmo.

Entonces lo que queríamos hacer es después de hacer un estudio para ver por qué hacer un estudio de caso para utilizar ECDSA a ver si la gente lo adoptaba. Recopilamos datos a través de una plataforma que se llama Open Intel. En la última diapositiva decimos que estés un proyecto de Surfnet, los

laboratorios SIDN y la universidad. Es una plataforma de medición de DNS de gran escala. Si les interesa este tema vengan hablarme después. Puedo explicarles un poco más. Los datos que usamos son datos de 3 gTLD: com, net y org. Y tenemos datos desde el primero de marzo de 2015 hasta el 14 de febrero de este año. Para punto NTL tenemos datos de un año y después para punto gov es un TLD muy especial. Tenemos datos de un solo día y también analizamos un solo día de datos de seis ccTLD, algunos de los cuales provienen de esta región.

En esta tabla... la diapositiva está en el sitio web de la ICANN. Entonces en la tabla pueden ver los datos estadísticos, pero pueden ver que hay distintos grados de adopción de DNSSEC. Punto NL tiene el valor absoluto más alto y también vemos donde está el valor relativo más alto. Creo que es el ccTLD noruego. Tiene un porcentaje levemente mayor. Pero todo está cerca del 50%.

La próxima diapositiva por favor. Entonces lo que queríamos hacer era ver la adopción de ECDSA. Vimos los identificadores algorítmicos DS, DNS key y RSSAC los registradores correspondientes. Hicimos una diferenciación entre implementaciones totales y parciales. Creo que lo que vemos acá es muy claro. Hay DNSSEC con firmas o no. Sí tenemos todos los ingredientes de DNS decimos que es una implementación total. De lo contrario es parcial.

Este es el gráfico de los tres gTLD más grandes. Lo que vemos aquí en pantalla esquela gráfico comienza el 15 de octubre porque antes de esa época casi no había adopción. Y lo que vemos acá es la fecha en que Cloud Flare anuncia DNSSEC universal. Durante casi un año fueron la única fuente de implementación importante de ECDSA en la firma de DNSSEC. Pero también es interesante observar que la parte azul más oscuro es implementaciones completas, la parte celeste son implementaciones parciales. Entonces el dominio está firmado pero no hay una delegación segura. Por lo tanto nadie puede validar las firmas. Después desde abril de 2016 es difícil leerlo en la pantalla pero alguien empieza a firmar sus dominios con ECDSA y esta es una compañía de medios que publica muchos periódicos locales en Estados Unidos. Son publicaciones como The Sacramento Bee.

Y las cosas después empezaron a ponerse interesantes a mediados de octubre del año pasado, cuando una compañía noruega, [incomprensible], pidió permiso para usar ese nombre suponiendo que no había ningún problema. Ellos activaron ECDSA para todos sus dominios. Creo que firmaron a todos sus dominios de manera predeterminada. Usaron ECDSA con todos los dominios. Lo interesante es que hicieron algoritmos. Firmaban como antes e hicieron algoritmos adecuados. Yo miré los datos de crecimiento, que los publicaron primero en las

firmas y después las claves, y tenían los dos algoritmos uno al lado del otro durante aproximadamente un mes y después pasaron totalmente a ECDSA. Lo que podemos ver es que ahora están yendo hacia la implementación de Cloud Flare.

La adopción parcial. La adopción parcial no curres solo para ECDSA, sino también para otros algoritmos. Abajo vemos la adopción de [incomprensible] uno y NSEC 3, que es el algoritmo 7, y vemos que es casi exclusivamente para despliegues. A la derecha es la adopción de RSA [incomprensible] 2 256, el algoritmo 8, dónde la mayoría de las instalaciones son parciales. Hay mucha gente que no firmó la delegación. Esto varía en las causas. Puede ser que el registrador no tenga soporte para la delegaciones seguras o que no soporte delegaciones seguras con un algoritmo en particular o que lo registratario simplemente se olviden de registrar las delegaciones seguras. Todas estas cosas parecen estar pasando.

Esperamos que con este nuevo uso de la clave la cosa cambie porque hay un reservorio importante de dominios reservados en TLD como punto com, que en este momento no pueden validarse porque no hay delegación segura. Esto va a aumentar significantemente el despliegue de DNSSEC en esos TLD.

La próxima. Esta imagen la tuiteé y también es un gráfico de la distribución de algoritmos en .com. Fíjense que el algoritmo

ECDSA PT56 en este momento está a punto de superar el RSA 256, que es bastante interesante. Parece ser que los nuevos despliegues del DNSSEC están comenzando a utilizar el ECDSA más que el RSA. Un poquito más preocupante es el enorme porcentaje de personas que siguen utilizando RSSAC, NSEC 3. No sé quién dijo, pero me parece que va a haber una charla sobre esto en Chicago. ¿Es así?

ORADOR DESCONOCIDO: Alguien tiene un draft, ¿no?

ROY: Hay dos drafts relacionados con este punto. Paul, quien me sigue, y yo hemos presentado drafts. Dos distintos discutiendo [incomprensible] uno y [incomprensible] 256 las actualizaciones.

DAN YORK: Creo que la idea aquí es alentar a la gente a que pase a [incomprensible] 256, que no usen el [incomprensible] uno.

ROLAND: La siguiente. No pude resistirme. Podemos hacer que ECDSA sea aún más grande, que sea inmenso. Sí, sí, sí. Me pueden odiar. Podemos hacerlo fantástico porque si cada dominio del

operador Cloud Flare desplegará DNSSEC universal, esto más que duplicaría el nombre de dominios firmados en org. Y de forma instantánea ECDSA serial algoritmo más utilizado en .com y .org.

Le voy a dar a Dan la oportunidad de mirar bien esta imagen, que se la puedo pasar si quiere. Creo que Oliver dijo que Cloud Fare tiene una política de hacer que la gente tome la decisión consciente de pasar a DNSSEC, el lugar de hacerlo ellos por sus clientes. Esta es una política que nosotros desde Surfnet no forzamos a la gente a usarla. Nosotros queremos este crecimiento orgánico al cual se refería Peter. Queremos que la gente pase sola por propia voluntad. Pero si todos lo hacen, si se les pudiera estimular, Cloud Fare fácilmente haría que ECDSA sea enorme.

Analizamos también la adopción de punto NL porque punto NL tiene el número más alto de dominios firmados, pero también no tiene soporte de ECDSA para delegaciones seguras. No lo tenía hasta marzo del año pasado. Entonces queríamos evaluar si había efectos después del despliegue en sus data sets. Los dominios punto NL firmados con Cloud Fare antes de la delegación segura, los que están arriba. Fíjense la flecha de arriba. Dice: más del 50% de estos despliegues parciales y asistían antes de la delegación y siguen siendo despliegues parciales hasta finales de año. O sea que la idea es que la gente

se olvida. Lo activa y se olvida de hacer la delegación segura porque yo chequeo los registros, a través de los cuales se registraron los dominios, y se olvidaron de registrar las delegaciones seguras.

Entonces en principio podrían convertirlo fácilmente en despliegues completos. Al principio solo los nombres operados por Cloud Fare usaron ECDSA, pero desde mediados de junio de 2016 otro operador comenzó a usar ECDSA. Más o menos al momento en que se liberó el de power. El algoritmo de ECDSA se empezó a utilizar más. Y fíjense que hay un par de hosts holandeses. Cada flecha apunta a un host individual que habilitó ECDSA para los dominios que ellos firmaron. Un buen observador notaría que la izquierda dice 8.000 dominios firmados con ECDSA. Si pensamos en los 2.600.000 delegaciones en punto NL es un número bastante bajo. Pero lamentablemente la gente avisó que es posible hacer una sobrecarga de algoritmos sin romper nada. Va a haber un traspaso de algoritmo, como para que la gente pueda aprender.

Analizamos otros ccTLD de Austria, Canadá, Dinamarca, Finlandia, [incomprensible]. No tengo idea de cómo se pronuncia, pero es una pequeñita isla en el Pacífico. Y Suecia. Las cosas varían. Por ejemplo Alexander de punto AT dijo ya la mañana que hace muy poquito que empezaron a soportar

delegaciones seguras para ECDSA. Y eso se refleja en el número de dominios firmados que han adoptado ECDSA, un 1%.

Ahora en el caso de Finlandia, el 75%. En Dinamarca el 80 y pico por ciento utilizan el ECDSA. Son números muy altos. Probablemente se deba a que son despliegues más recientes. Entonces la gente mira la documentación antigua, dice: "bueno, quiero hacer despliegue, quiero también que las respuestas de DNSSEC sean considerables". Entonces hace delegación segura.

Luego analizamos punto gov. Los organismos federales tienen que firmar sus dominios punto gov. Hay una directiva presidencial del 2009 que establece: usted deberá firmar el dominio Federal. Y el [incomprensible] recomienda utilizar ECC y también recomienda que si la gente usa claves RSA que sean más grandes. Entonces nos preguntamos: ¿los dominios punto gov usan ECDSA? Y la respuesta es no. Ni uno. Cero. Y otras cosas divertidas...

DAN YORK: ¿Puedo hacer un comentario? no hay forma de subir las claves ECDSA debido al registro.

ROLAND: Eso no lo sabía. Es más divertido. 8% de los dominios punto gov utilizan exclusivamente claves RSA de 1024 bits. ¿Quién hablaba

de los recortes presupuestarios? Paul. Y de no reemplazar los equipos. Seis dominios punto gov utilizan todavía RSA de 512 bits y casi el 50% de los dominios punto gov utilizan hashing [incomprensible] uno, a pesar de las recomendaciones de [incomprensible] de dejar de hacerlo en el 2015.

ORADOR DESCONOCIDO: Es un problema porque el traspaso no es algo que se hace con un solo clic.

ROLAND: No es excusa. Punto gov es uno de los primeros esfuerzos serios para que DNSSEC se instale en el espacio gubernamental, pero están gravemente atrasados. Es una gran preocupación. No le he pregunté a Scott Rose qué opina, pero me parece que no está muy contento.

ORADOR DESCONOCIDO: La semana que viene en Chicago le podremos preguntar. Si lo veo se lo preguntaré.

ORADOR DESCONOCIDO: No quiero que quede claro echar la culpa o avergonzar a punto gov porque hubo un esfuerzo importante originariamente. Solo digo que debes de seguir prestando atención si hacen DNSSEC.

Era una tecnología nueva cuando comenzaron a desplegar la y yo diría que cosas como ECDSA, DANE es una tecnología más madura pero que hay que seguir actualizándola.

DAN YORK: Ahora tenemos nuevas curvas, Todos los EDDSA, la gente que hace cripto lo quiere cada vez más porque es un nivel de seguridad superior a ECDSA. Entonces los [incomprensible] van a llevar aún más tiempo.

ORADOR DESCONOCIDO: En un trabajo preliminar que hicimos demostramos que junto con la clave de firma combinada tiene ventajas adicionales a la hora de reducir la fragmentación y la amplificación porque las respuestas de firma son específicas o podemos tener respuestas con amplificación y eso hay que reducir el tamaño de las respuestas.

ECDSA, o incluso EDDSA, cuando estén disponibles en las implementaciones y habrá reducido el tamaño significativamente, pero el uso de una única clave ayuda a disminuir el tamaño de lo que se tenía antes. Entonces nos preguntamos: ¿La gente utiliza las claves combinadas con ECDSA? Y lamentablemente la tendencia no fue clara. Parece ser de todo un poco. En algunos ccTLD ahí números importantes de

dominios que utilizan clave combinada, pero en .com y .org no hay ningún adopción de esto.

Esto es algo que la gente tiene que empezar a considerarlo. Miro a [incomprensible]. O sea, ECDSA con clave combinada. Los usuarios que pasaron a ECDSA tendrían este esquema. Por supuesto si hablamos de DNSSEC es interesante ver el pasado y ver qué pasó con RSA. 1024 bit hoy día es considerado como muy débil. La gente se recomienda que pase a claves más grandes. Ahora, ¿lo hace así la gente? ¿Cambia?

Veamos los números para .com y .org. En estos tres el 40% de los despliegues que utilizan RSA tienen clave de 1024 bits. Son números importantes. Algo también interesante y que por algún motivo la gente piensa que las claves RSA solo vienen en potencias de 2. Es decir, si teníamos 1024 antes teníamos que ir a 2048, y de 2048 tendremos que pasar a 4096, qué es el tamaño más alto que se permite en DNSSEC. Entonces la gente que usa RSA tiene una clave que no es una potencia de 2. En gTLD esto es números negligibles.

En punto NL no es negligible. No es despreciable pero es bajo. Si de alguna manera pasarán a DNSSEC, que por un tiempo sigan con RSA, pero quieren actualizar seguridad, el software no puede manejar claves que no son potencias de 2, como para no arruinar la respuestas. La siguiente.

ECDSA, como decía, se ha estandarizado hace muy poco gracias a Andre y Robert con dos curvas, la ED 25519 y la ED 448. Es muy atrayente la ED 25519 porque solo porque solo requiere 32 bits instalados en un registro de DNS key. Es la representación de la curva completa, que se necesitan 64 bites en un registro DNS. Pero afortunadamente ECDSA utiliza compresión que no está patentada. O sea, que se puede almacenar como una única parte de la representación del punto de la curva y se puede almacenar claves incluso más pequeñas en el registro.

Y el ED 448 también se estandarizó. Es una curva de alta seguridad que hay que utilizar si hay requisitos de muy alta seguridad. Yo creo que la curva de 256-bit cubre las necesidades. Sí unos paranoide hay que ir a la curva de 448 bit. Pero con la de 256 estaríamos cubiertos en casi todas las aplicaciones.

Como EDSA es nuevo, no está basado en ningún software. Pero hay razones para promocionar su soporte. Es mucho más rápido que ECDSA. Requiere menos espacio y tiene mejores propiedades de seguridad. ECDSA tiene algunos problemas de seguridad. La gente que desarrolló EDDSA tiene una lista de las medidas de protección que cuenta cuáles son las propiedades de seguridad mejoradas y lo que yo quiero hacer ahora es pedir a la gente que exprese su apoyo al proyecto OS para

implementar EDDSA porque así vamos a hacerlo mucho más rápido que lo que lo hicimos con ECDSA.

Y ahora estamos renovando nuestra infraestructura con nuevos HSM, donde almacenamos las claves. Y los alentamos a los proveedores a dar apoyo a EDDSA. Ellos dicen que lo tienen en su hoja de ruta. Esperemos que los HSM tengan soporte pronto. La próxima.

Para concluir, el Gráfico mostró que la adopción de EDDSA ya se ha iniciado en algunos sitios como .com y .org. Vemos un número significativo de dominios firmados con EDDSA. O sea, qué vemos que está superando algunos algoritmos RSA, pero los algoritmos están disponibles sólo para un puñado de operadores. O sea, la gente que pasó en grupo, a granel, conté que son unos 50 operadores grandes los que activaron. Pero también hay muchos operadores grandes que siguen con RSA y en el caso de com y org con 224 bits. Las delegaciones seguras a través del canal RRR bloquean el despliegue de DNSSEC en general. La próxima.

Ahora para todos aquí en la sala pregunto: Si uno es un operador y planea un nuevo despliegue, por favor firme el ECDSA. Considérenlo. Si bien es algo trivial, la gente ha demostrado que es algo definitivamente posible. Lo vamos a hacer en el 2017 nosotros. Si ustedes hacen validación de

DNSSEC comprueben que hay soporte para ECDSA. El 80-85% tienen validación, pero no el 100. Así que nosotros queremos el 100%.

¿Qué vamos a hacer nosotros? Vamos a pasar a ECDSA PT56 con una clave combinada. Ese esquema de clases combinadas para aquellos que emigran a clientes. Vamos a migrar a nuevos HSM. Vamos a hacer el traspaso del algoritmo. No son muchos dominios. Son solo 1200. Creo que somos un operador pequeño en ese sentido, pero trataremos de compartir las experiencias. Haremos un blog sobre nuestro progreso, compartiremos los script y el código de automatización, como para que la gente aprenda. O sea, vamos a abrir el DNSSEC. Vamos a compartir los script, como un DNSSEC abierto.

Va a haber un soporte del traspaso en el software. O sea que si quieren pasar a un nuevo algoritmo, eso fue lo va a permitir, en lugar de tener que hacer un script molesto. La siguiente.

Bueno, esto es para referencia. Las diapositivas estarán disponibles si quieren leer más. Algunos vínculos aquí tienen. Bueno, eso es todo. Quiero agradecer a la gente de ISDN, a Intel por los datos que usé en esta presentación. Si tienen preguntas aquí estoy.

DAN YORK: Veo que ya hay una fila de personas que quieren hacer preguntas. En primer lugar gracias, Roland, por este trabajo. Muy buenos números, muy buena información. Gracias por haberla organizado. Veo a Paul, Jacques, Peter. Paul primero.

PAUL: En una de las diapositivas dijo que EDDSA es más rápido. Supongo que eso es para la firma, ¿qué es mucho más rápido?

ROLAND: Tanto para la firma... Si me dan un minuto les puedo dar los números.

PAUL: Esa era mi segunda pregunta. Hicieron un muy buen desglose de la información explicando por qué funcionaba mejor del lado del resolutor. ¿Tienen números de performance para EDDSA?

ROLAND: Sí. Lo tengo. ED25519 en términos de velocidad de validación si lo comparamos con uno punto dos, que tienen los parches, requiere un 70% de tiempo de CPU para hacer la validación. Así que es un 20% más rápido. Y ED448 es solo dos veces más lento que ECDSA P256. Si lo comparamos con el 4 es más rápido. 224 es 4 veces más rápido que P84 y da más seguridad.

ORADOR DESCONOCIDO: Quisiera saber si tiene datos sobre TLD. Cuántos dominios firmaron con EDDSA. Sé que en punto CZ tenemos muchos.

ROLAND: No tengo los datos acá pero sí los tengo. No los puse en la presentación.

CARSON: Roland, muy buenos datos. Tengo una pregunta para todos, no solo para Roland. La última vez que hice un rollover del algoritmo tuve que realmente meter las manos en eso, ensuciarme con eso. ¿Cómo está el soporte para software con DNSSEC? Quizás hay algunos acá que puedan aclararme esto porque en este momento es muy difícil hacerlo. No es imposible, pero es difícil qué es un algoritmo de traspaso.

DAN YORK: ¿Tiempo de hacer un comentario?

ORADOR DESCONOCIDO: Yo estaba más cerca del micrófono, así que contesto primero. Voy a aprovechar esta oportunidad para predicar un poco.

Es un problema que tenemos. ¿Cómo es el problema? Tenemos la industria de hosting. Todos usan nuestro software, que escribe muchos de los que están acá. Y vienen con preguntas como está. Por ejemplo, ¿podemos hacer el traspaso de la clave agregando la nueva clave con la nueva línea de comando y después dejar de ejecutar la línea de comando para sacar la clave vieja? Entonces manualmente uno lo puede hacer. Hace falta código para que esto ocurra. Nos encantaría mejorar esto. Está nuestra hoja de ruta. ¿Ustedes saben cuántos proveedores de hosting apoyan nuestros desarrollos? Es como la implementación de ECDSA con punto gov. Es cero. En esta sala nos encanta hablar acerca de que la comunidad de los operadores es lenta y no nos acompaña, pero ellos apoyaron el desarrollo de los servidores de nombre.

Entonces aun cuando vuelcan muchos dólares o euros por dominio por año, cuando les pedimos que financien este desarrollo para simplificar la vida dicen: "No, nosotros nunca pagamos nada en esta empresa y no lo vamos a hacer ahora". Para redondearlo me encantaría automatizar el traspaso. Creo que no sería difícil hacerlo, pero me enfrento con la perspectiva de implementar esto para gente que no contribuye con código, no contribuye con esfuerzo y tampoco con dinero. Entonces me encantaría simplificarlo, pero quisiera saber si aquellos que

alojan millones de dominios podrían apoyar un poco este desarrollo de software. Gracias.

DAN YORK: Esto es normal en general. Esta persona acepta dinero y designaciones. Los parches también. Parches, códigos, fondos para códigos. Peter. ¿Quién habla primero?

PETER: Quería agradecerle a Roland por esta excelente presentación y por el trabajo detrás de eso. Tengo una o dos preguntas o comentarios. En primer lugar por supuesto que está esta división interesante de uno K, dos K. Y la gente interesante al parecer solamente piensa en dos. Cuando usted mencionó la clave combinada, ¿no sería natural que alguien que tiene una división de uno K o dos K siga con la clave combinada de uno K? Porque esa es la fortaleza del superset, por así decirlo.

ROLAND: No sé por qué lo harían pero poca gente utiliza la clave combinada. No vi una gran implementación de esto punto DL lamentablemente.

PETER: Hice este comentario porque me preguntaba: Cuando el registrador tienen todas sus manos, incluido el traspaso de la clave a través del sistema de registración, ¿por qué lo va a dividir? Mantener RSA...

ROLAND: Porque nosotros les dijimos en un RFC 4641 que tenían que tener la clave dividida. Eso les motivó.

PETER: Pero la actualización 6781. Pero seguir con RSA, pasar a clave combinada y después pensar solamente en potencias de 2 esto probablemente va a tener un efecto interesante sobre el tráfico saliente, por lo menos creo que la gente debería saber esto.

En cuanto al lado del ECDSA, me encantaría ver el apoyo de los proveedores para los HSM, para estas nuevas curvas. Nosotros hicimos un ejercicio el año pasado y creo que tuvimos una respuesta similar. Sí, sí. Lo vamos a poner en nuestra lista de cosas por hacer, pero lo que nos dijeron los proveedores fue que esto por supuesto es mucho más difícil que agregar otra curva del tipo ECDSA porque es necesario tener todos los cálculos matemáticos, etc. Y quizás se pierda o no la certificación. Ahora acá viene la trampa de cumplimiento. Sí uno tiene que cumplir con el requerimiento de utilizar algoritmos que tengan un

determinado sello de certificación porque uno está regulado o lo que fuera, entonces estamos en problemas. No podemos innovar. Y eso es malo para los reguladores y los legisladores que deben saber esto.

Ahora con respecto a EDDSA, no lo mencioné pero quizás sea interesante para algunos miembros del público saber que no necesitan, que puede utilizar firmas reproducibles, lo cual es interesante en situaciones de la redundancia. Quizás no sea importante para todos los casos, pero sí para grandes instalaciones.

ROLAND: Sí, no quise entrar en demasiados detalles porque hace falta saber bastante con respecto a cómo funciona ECDSA. Me cuesta a mí así que imagino que los demás también. Pero hay dos implementaciones. Se puede utilizar una cadena de entrada aleatoria, que sea totalmente aleatoria, pero también hay un RC que nos da una forma determinista de general esto e incluirlo en la firma.

Entonces podemos hacer firmas deterministas con ECDSA. De hecho si hacemos ECDSA probablemente sea la forma más segura de hacerlo porque si de alguna forma generamos dos firmas y reutilizamos los mismos números entonces la clave

privada se puede recuperar. Es un tema de seguridad serio con ECDSA.

DAN YORK: Bueno, acabamos de escuchar mucha información encriptada. Estamos entrando la zona de expertos.

ROLAND: Por eso no lo mencioné antes.

DAN YORK: Sí, sí, sí. Estamos hablando sobre temas sumamente técnicos criptográficos, pero supongo que todos los que están a casa ven que esta era una sesión técnica y si no, se lo acabamos de demostrar. ¿Hay otras personas que quieran hablar? Irwin.

IRWIN: Quería confirmar sus sospechas acerca de DK. Hay algunos nuevos hosts que se incorporaron, algunos nuevos registradores que se incorporaron en los últimos meses. Nos acercamos casi al 1% del porcentaje de nombres de dominio. Hicieron un traspaso de algoritmo.

DAN YORK: Es fantástico ver lo que se puede hacer en ese sentido, en cuanto hacer esta clase de cambios.

OLIVER: Roland, muy bueno. Quería tomármelas con usted un poco.

ROLAND: Adelante.

OLIVER: Usted dijo que mis clientes están en un Estado muy inicial, pero ¿qué pasa en el resto del mundo? Porque si vemos los dominios que son operados por los que no son registradores es un problema muy serio hacer llegar el material y hacerlo pasar por la cadena.

ROLAND: No quise tomármelas con Cloud Flair. Si se interpretó así le pido disculpas. Pues solamente un ejemplo. De hecho, realmente agradezco que usted haya escrito el RFC. Muy bueno.

OLIVER: Jacques, Paul y yo tratamos de incluir un protocolo en el mundo regulatorio y queremos hablar también con los registradores para que carguen la información de una forma estandarizada

para que todos lo hagan de la misma manera. Pero también ahora quiero tomármela con Dan. Sus fantásticos comentarios acerca de que publica todos los lunes. Quizás podría empezar también a mostrar datos parciales y no solamente los datos que publica los lunes.

DAN YORK: Quizás voy a tener que hablar con alguien acerca de los fondos, del financiamiento para el [incomprensible] del código.

OLIVER: Es solo código.

DAN YORK: En serio los mapas de DNSSEC es código que nosotros tomamos de [incomprensible]. Yo sé que usted trabajo con este código. Estamos abiertos a ampliarlo, expandirlo, y hacer más. ¿Cuánto? Es una cuestión de ciclos, el tiempo. Alguien debería poder trabajar en esto.

Bueno, de todas formas ¿hay alguna pregunta o comentario antes de cerrar la lista de personas?

MARCOS: No sé, y quisiera recibir una respuesta práctica para un caso de uso real. ¿Puedo firmar mi zona utilizando el algoritmo ECDSA

más avanzado? ¿Qué pasa si el resolutor no puede entender la firma? ¿Va a decirle al cliente que no está autenticado? ¿Es eso lo que cabe esperar? ¿O se va a romper algo?

DAN YORK: Correcto. El RFC dice que si el resolutor de validación no conoce el algoritmo, debe enviarlo sin firmar. Una respuesta de no firma.

ROLAND: La gente de APNIC, George y Jeff, analizaron esto y creo que vieron que este comportamiento es el que se implementó. Eres lo peor es que se quiebran porque no tienen el algoritmo. Simplemente nos dan una respuesta no validada.

DAN YORK: Además en una de las listas de mailing surgió una excepción a este caso. Alguien mencionó que hizo el traspaso con una versión de lo que estaban usando en el CPE. Estaba mal configurado.es decir, fallaba. Pero terminaron con...

ORADOR DESCONOCIDO: Con dos versiones de DNS mask.

DAN YORK: Sí, básicamente no lo implementó. Falló. No conocía al algoritmo. Decía está firmado pero no sé cómo resolverlo, así que chao.

Esto después se reparó. Así que ahora ya no lo está haciendo. Pero durante un tiempo sí vimos el comportamiento equivocado. Sin embargo con respeto ese punto, quiero decir que estamos hablando mucho de EDDSA, pero tengo una pregunta breve. Lo estoy mirando a usted, [incomprensible], y a otros. ¿Dónde están ustedes? ¿En qué punto están ustedes con respecto a poner esta disposición de unbound y otros?

ORADOR DESCONOCIDO: Está en nuestra hoja de ruta. Lo vamos a implementar pronto. Por supuesto, todavía está en la biblioteca de seguridad. Habrá una versión pronto.

ORADOR DESCONOCIDO: Esta mañana dije que estamos esperando que el nuevo DNS lo soporte. Y en cuanto lo soporte lo vamos a implementar inmediatamente.

DAN YORK: Volviendo al punto que señalamos antes, financiamos desarrollo y proyectos de código abierto sobre este tema.

¿Alguien más quiere hacer un comentario? Habiendo dicho esto, quiero agradecerle a Roland por todo su trabajo.

Y ahora si les parecía que no estábamos muy metidos en lo técnico, vamos a pedir a Wes que nos lleve a descender introducirnos en el gran ejercicio de preguntas y respuestas de DNSSEC. Mientras viene Wes, vamos a pedirle a Julie. ¿Quiere hablarnos sobre el almuerzo?

JULIE: Sí, primero quiero que busques en la hoja que les estoy mostrando con las preguntas y respuestas de este ejercicio. Deberían tenerlo en la mesa. Wes les va a dar las instrucciones y les va a decir lo que tienen que hacer. Vamos a hacer una pausa para el almuerzo después de responder este cuestionario. Tenemos una cantidad determinada de espacio para el almuerzo. Por eso antes les dimos las invitaciones. Lo van a necesitar para ingresar en la sala donde se va a servir el almuerzo. Todavía quedan algunos tickets que están sobre las sillas, así que miren a su alrededor.

Nos quedan algunas más pero muy pocas, así que fíjense primero si no quedaron algunos en las sillas. Eso es todo. Wes, le doy la palabra.

WES: ¿Cuántas personas estuvieron en Hyderabad y respondieron el cuestionario e hicieron este ejercicio? ¿Cuántos de ustedes obtuvieron un resultado negativo? Excelente. Pasamos a la próxima.

Les agradará saber que esta vez no he resultados negativos, así que les garantizo que todos van a tener un puntaje positivo. Y no digo cero. Digo positivo.

Vamos a ver algunas reglas breves. Para ser declarado ganador, alguien que esté al lado de usted tiene que haber validado su respuesta. Es decir, para competir para ganar el campeonato tiene que asegurarse de que alguien valide o convalide y corrija su respuesta. Cada respuesta correcta vale un punto. Las múltiples respuestas a veces es correcto que haya múltiple respuestas, pero sigue una respuesta incorrecta entonces para esa pregunta tendrá un valor de 0. A veces es bueno elegir varias respuestas y a veces no. Si elige una respuesta incorrecta, el valor para esa pregunta va a ser 0. Y finalmente yo, Wes, siempre tengo razón aun cuando me siento mal como ahora, pero todavía la mente me funciona bien.

Entonces primero, pregunta cero. ¿Qué cosa rica de chocolate en Dinamarca está prohibido importar a Estados Unidos? ¿Kinder surprise, Kinder surprise o Kinder surprise? La sorpresa de kinder. Le vamos a dar un premio al ganador. Este huevo de

chocolate extremadamente peligroso no puede importarse a los Estados Unidos porque tienen piezas con las que uno se puede atragantar. Así que por favor no lleven este huevo de chocolate a Estados Unidos si ustedes son de ahí.

Pueden ver qué acá las 4 respuestas son correctas. Si ustedes marcaron las 4 o respuestas como correctas regalaron 4 puntos. ¿No es muy bueno eso? Soy tan bueno. Esa fue la pregunta cero.

No coordine con Julie acerca de coordinar esto. Mala mía. Y tampoco quería tener que acordarme de todas las diapositivas.

Pregunta 1. ¿Cuál de los siguientes ccTLD comenzó a cumplir totalmente con DNSSEC en diciembre de 2016?

PETER: ¿Puedo hacer una pregunta? Me parece que uno de estos está en la lista de uso especial del IETF.

WES: Pluto. Te ganaste un punto. Hong Kong, Sudáfrica, Vietnam, punto HK, punto CA, punto VN. Y por supuesto Plutón.

Pregunta número 2. ¿Vamos bien? sí. Vamos a la pregunta número 2. ¿Dónde tuvo lugar la primera ceremonia de la clave para la creación de la clave para la firma de la llave de la raíz? fue a) california; 2) Culpepper, Virginia; c) París, Francia; o d)

Plutón en la vía Láctea. La ceremonia de la clave no puede tener lugar en dos lugares al mismo tiempo, así que acá tienen que elegir una sola respuesta. Me estoy portando muy bien con ustedes.

Este es un tema general. Pronto vamos a hacer el traspaso de la KSK, así que todos pueden participar. Espero que hayan estudiado todo porque se miraron las diapositivas de Matt y de otros oradores les va a ir mejor en este cuestionario.

La siguiente. Pregunta número 3. ¿Cuándo se espera que se revoque la KSK actual? Eso directamente estaba en la diapositiva de Matt, así que espero que hayas memorizado todas sus diapositivas porque es a) 11 de julio de 2017, b) 11 diciembre de 2017, c) 11 de enero de 2018, d) 13 de enero de 2018. Es una de esas fechas.

Es la clave que está en este momento vale ida. Si todo funciona bien es la fecha de bajada digamos.

La siguiente pregunta. ¿Cuál es la duración mínima o el tiempo mínimo que ICANN tiene que esperar después de publicar la nueva KSK de la raíz del DNS para esperar que todos los validadores en línea confíen en la nueva clave? No sé si la semántica de esta oración es correcta, pero está basado en un borrador, en un draft que yo redacté, así que van a tener que leer mi documento para entender esto. Es a) 30 días, b) 45 días,

c) 61 días y medio, o d) 365,25 días. Eso es lo que ICANN tiene que esperar antes de considerar que todos los validadores en que en cumplimiento de la RFC 5011 confían en la clave. Ustedes fueron los responsables de los números estos, así que la culpa es de ustedes.

La pregunta 5. ¿Qué propiedades se corresponden hoy día con la zona raíz firmada de DNSSEC? NSEC ZSK de 1024 bit y RSA [incomprensible] uno; b) O B, NSEC ZSK de 2048 bit; c) NSEC tres con 1024 bit; d) NSEC con 2048 bit y RSA [incomprensible] uno; o e) TLS v3.1 y [incomprensible] uno con prop tres.

La que sigue. Pregunta 6. ¿ cuál de los siguientes registros ccTLD tiene registros DS en la raíz hasta la fecha de ayer? a) punto AC, punto BE, punto CF, punto DK; b) punto AD, punto BW, punto CN, punto DK, Dinamarca. Vamos a tener que dar los regalitos porque están en todas las respuestas Dinamarca. c) AE, BG, CC y el anfitrión Dinamarca. d) AF, BH, CR y DK. Si ha memorizado la raíz recordarán que www, xx, yy y zz no existen, pero si existen lo pueden poner igual.

La que sigue. No, vamos para atrás. No se puede usar las computadoras ni buscar nada en internet. Eso es hacer trampa. 4, 3, 2, 1. De vuelta atrás. La siguiente. Pregunta 7. Aquí es donde conseguirán muchos puntos si conocen muy bien el protocolo. Escriban cualquier flag de encabezado de DNS o EDNS

registrado con IANA, la abreviatura de 2 letras y también los nombres de expansión. Por ejemplo, el bit do qué representa DNSSEC okay. Pónganlo. Ya aprovechen porque es una de las respuestas. Esa es la pregunta 7.

Queda una pregunta más. Completa en lo después cuando quieran. Pasemos ahora a la siguiente pregunta. Pregunta 8. ¿Cuáles son los IDS clave de 5 dígitos de las claves activas de la zona raíz hoy? Si conocen los key ID, como todos lo conocen por supuesto, lo escriben. Pueden adivinar. Son 5 dígitos.

ORADOR DESCONOCIDO: De las dos claves activas hoy día para el traspaso en este momento hay una sola ZSK activa.

WES: No importa porque es la que se va a firmar, la que se está firmando. ¿Por qué no volvemos a la pregunta 7 para que la gente pueda responder? Porque la otra era la última. Les doy unos segunditos.

Hubiera hecho algo mejor pero me sentía mal anoche. Espero que esté bien esto.

JULIE: Era un formulario, una plantilla ya armada. No anticipaba.

WES: Era un cero. Nos volvimos a la pregunta 7 para que puedan volver a leerla. No hay dos preguntas 7. La última pregunta era la 8. 2 letras.

No, gracias, Paul. Tanto para esta como para la que habla del ID, del key ID, la última, tienen permitido adivinar. Entonces si sacan tres mal. Por ejemplo, AQ para [incomprensible], lo pueden poner.

Hay personas que están todavía escribiendo. Paul, les vamos a dar tiempo. A mí me costó trabajo encontrar una sigla de 2 letras en un caso. Se acaba el tiempo. Roy, escribo más rápido. Paul también terminó así que creo que ya está.

Julie, ¿podemos seguir? Recuerden que para calificar para de premio tienen que pasarle la hoja a otra persona que les dará la nota, el puntaje. No tiene que ser nadie de confianza para que no les ayude. Al final les voy a preguntar quién les corrigió la prueba. Pasemos a las respuestas, Julie.

Pregunta cero. Sí pusieron kinder surprise ganaron 4 puntos. Felicitaciones. La siguiente. ¿Cuál de los siguientes ccTLD obtuvo el cumplimiento pleno con DNSSEC en diciembre de 2016? Las tres. Espero que no hayan puesto Plutón porque esto invalidaría la pregunta por completo.

Las diapositivas decían diciembre. ¿Recuerden que la primera decía que yo siempre tengo razón? Así que en realidad no importa lo que realmente paso. Les voy a dar un crédito porque esto lo leí estando enfermo anoche, así que decía diciembre.

ORADOR DESCONOCIDO: Estás equivocado. Oh, no. Tienes razón. Es el 16 de diciembre.

WES: Les dije que siempre tengo razón.

ORADOR DESCONOCIDO: Añadir a la zona no alcanzan.

ORADOR DESCONOCIDO: Esto se interpone entre nosotros y el almuerzo, así que ¿por qué no avanzamos?

WES: La siguiente. ¿Dónde fue la primera ceremonia? Culpepper, Virginia. El segundo fue la segunda ceremonia. Pregunta 3. ¿Cuándo se espera que se marque como revocada la clave actual? El 11 de enero de 2018. Pregunta 4. ¿Cuál es el tiempo mínimo que ICANN debe esperar después de la publicación? 61 días y medio. Ahí están los números, Warren. Léelo.

ORADOR DESCONOCIDO: No, eso es para los validadores en línea. Si el validador está fuera de línea... Por eso dice online. Está ahí. Tercer renglón.

WES: Tienes razón. La siguiente pregunta 5. ¿Qué propiedades se corresponden hoy en día con la zona raíz? B) NSEC ZSK de 2048 bits, que es nuevo. No hace mucho tiempo. Y RSA [incomprensible] 256. La siguiente. ¿Cuál de los siguientes ccTLD tiene registro DS en la raíz? Es la superior. AB, BW, CN y DK. Fíjense que los que están en rojo no están. No tienen registros. Hay uno para CN. Anoche lo hice. Lo acaban de revocar.

ORADOR DESCONOCIDO: Dice diciembre de 2015.

WES: Debo de decir que Rick me mostró un registro que sí existía.

¿Qué decía la diapositiva número 2? Decía que yo siempre tengo razón. Está usando un resolutor que anda mal.

ORADOR DESCONOCIDO: El almuerzo, Wes.

WES: Pregunta 7. DNS y EDNS registradas con IANA. No sé si están calificando, pero tienen que saber AA, que es authoritative answer. TC respuesta truncada. Si pusieron alguna otra cosa truncada no vale. Tiene que decir respuesta truncada y TC. RD, recursion desired. RA, recursion available. AD, authentic data. Not authenticated data, datos auténticos. No autenticados. CD, checking disabled, comprobación inhabilitada. Y el que les dimos, el do, que es DNSSEC okay.

ORADOR DESCONOCIDO: Falta uno ahí. El QR.

WES: Tiene que decirle a la IANA porque esto lo saque de su página. Existe pero hay que decírselo a la IANA.

ORADOR DESCONOCIDO: Veo que la IANA por el orador que está ahí atrás se notifica.

WES: Siguiente pregunta. ¿Cuáles son los key ID? Volvemos atrás. El bit do no es lo mismo. Acepto la misma respuesta la siguiente. Por último, la pregunta. Las claves son 1936 para KSK y 61045 para ZSK. ¿Quién puso los dos?

ORADOR DESCONOCIDO: Yo puse múltiplos.

WES: Es una respuesta incorrecta. Felicitaciones. ¿Eso es todo?

Creo que la próxima no tiene nada bueno. Pasen las hojas calificadas a su compañero con el puntaje y comenzamos. ¿Alguien sacó menos de cinco? Porque si no, no siguieron las instrucciones. ¿Preguntas? No. ¿Quién sacó más de ocho? Varios sacaron más de 8. ¿Quién sacó más de 9? Entonces estas personas sacaron por lo menos 10. ¿Quién sacó 11 o más? Quedan menos de este lado. Este es el panel de expertos aparentemente. ¿12 o más? 13. ¡Ah! El huevito kinder. Lo voy a ir a buscar. Esto es ejercicio. 14. Bueno, se lo dejo a Paul y a Warren para que ellos vean cómo lo parten. Recuerden que hay objetos pequeños con los cuales se pueden ahogar. Tengan cuidado. Así que gracias a todos y que se diviertan.

ORADOR DESCONOCIDO: Gracias, Wes. Bueno, el almuerzo es en la sala C1.1. En el ticket hay un mapa pueden ir por la alfombra azul y doblar a la derecha. Si no tienen ticket y quieren participar nos quedan algunos. Vengan a verme y se los doy. Vamos a reanudar en esta sala a las 13:45. Esa es la idea. En aproximadamente 40 minutos.

[FIN DE LA TRANSCRIPCIÓN]