ABU DABI – Taller sobre el DNSSEC – Parte 2
Miércoles, 1 de noviembre de 2017 – 10:30 a 12:00 GST
ICANN60 | Abu Dabi, Emiratos Árabes Unidos

ORADOR DESCONOCIDO: ¿Podemos empezar ya?

RUSS MUNDY: Muy bien. Estamos por recomenzar. Tenemos nuestro próximo panel. Vamos a cambiar un poquito el orden de lo que había en nuestro programa. Muy bien. Duane está por ahí. ¿Por qué no viene para aquí, para que esté un poquito más visible? Duane es el que va a hablar primero. Luego lo van a seguir Akkerhuis y Cristian Hesselman. Luego la gente de ARIN y de ICANN. Creo que tenemos suficiente tiempo aquí para hacer una sesión de preguntas y respuestas en cada una de las presentaciones. Vamos a recibir preguntas entonces con las presentaciones. Ahora le doy ya la palabra a Duane.

DUANE WESSELS: Gracias. Agradezco poder ser el primero. Esta presentación es sobre la RFC 8145. Mi interés es tanto como coautor y también como persona que recibió alguno de los datos. Esta es una versión breve de la charla que di en la DNS-OARC, que contiene las partes principales. Esta RFC define el proceso a través del

cual los validadores pueden señalar sus conocimientos de anclaje de confianza. La señal tiene una forma de una etiqueta de llave y allí hay dos etiquetas que son válidas. Una es la 19036 para lo que llamamos KSK 2010 y 20326 para el KSK 2017. Estas señales se reportan a los servidores de nombre autoritativos en la zona. Los validadores deben transmitirlos a través de un TTL. La RFC define dos formas de key tags. Una es a través de la opción EDNS 0. Todos los datos vienen en la forma de este segundo formato, que es un query key tag donde los datos están codificados en el nombre de la consulta y los valores están codificados en hexadecimal. Uno es 19036, que es para 4A5C y 20326 es para 4F66.

Esta tabla muestra el cronograma de cómo se fue implementando. El primer borrador fue en diciembre de 2015 y para el 2016 ya había una implementación en BIND. Luego hubo otro borrador que se convirtió en la RFC 8145 en abril y, al mismo tiempo, hubo una implementación en Unbound. Mayo fue el momento en el que empecé a mirar los datos. En BIND esta característica se permitió por default y en Unbound no fue inicialmente por default sino que cambió a default en octubre.

Vamos a ver ahora algunos datos. Como dije, la señal se envía a los servidores de la zona raíz. Estos datos provienen de la raíz A y la raíz J. Lo que quiero dejar en claro es que estos datos provienen de una implementación reciente de software de

nombre de servidor. Solamente aquellos que actualizaron son los que nos dieron estos datos. Esta diapositiva muestra cómo se ven los datos en crudo. Aquí hay un sello de tiempo con el nombre de query donde vemos TA y los dígitos hexadecimales, origen, la dirección de destino también. En la mayoría de las columnas de aquí mostramos solamente los anclajes de confianza anteriores. La mayoría de estas líneas tienen solamente eso para 4A5C y ambos valores indican que estas son fuentes que ya tienen el KSK nuevo.

En este gráfico vemos la cantidad de fuentes que dan los datos, las direcciones de IP que los datos por día durante un periodo de tiempo. Esto comienza en mayo y continúa hasta hace poco tiempo. La primera línea vertical a la izquierda marca el tiempo en el que el KSK 2017 se publicó por primera vez en la zona raíz y la segunda línea en vertical a la derecha indica el tiempo en el que la RFC 5011 está en un tiempo en el que funciona. Luego agregamos una nueva llave al anclaje de confianza. Inicialmente teníamos 500 fuentes por día y ahora estamos en 2.500 por día.

Este gráfico nos muestra cuáles son las señales que esas fuentes están enviando. De nuevo, esto es por día. El rojo, a la izquierda, indica señales que muestran solamente los anclajes de confianza de 2010. Lo que está en verde a la derecha son las fuentes que tienen tanto 2010 como 2017 en lo que se refiere a anclajes de confianza. Quizá es un poco difícil de ver pero entre el verde y el

rojo hay unos píxeles de amarillo que representan las direcciones IP fuente que en el transcurso del día envían señales de bits. A veces se dice que tienen la llave vieja y a veces se dice que tienen tanto la llave nueva como la vieja. Es un porcentaje bastante reducido.

Lo que era preocupante antes del rollover es que lo rojo estaba muy bajo y no bajaba más. Estaba como plano. Van a ver que vemos también una subida en algún punto. Estos son los mismos datos que están representados como porcentaje. Se puede ver que después del tiempo del timer de hold-down una gran parte de los validadores indicaron que aceptaron los nuevos anclajes de confianza y continuaron.

No tengo un clicker aquí pero si miran abajo a la derecha, hacia fines de octubre, van a ver un pequeño aumento. Las indicaciones preliminares nos dicen que esto se debe al software Unbound. Unbound publicó una versión el 10 de octubre con los datos de anclaje de confianza por defecto y pareciera que esa población que está utilizando Unbound tiene una gran cantidad de personas que todavía no tenían la nueva llave.

Otra cosa interesante para ver es cuántas veces vemos datos inesperados o que no son de IANA. Desde el principio de la colección, yo veo unos 29 key tags. Muchos más de los 19 que esperábamos inicialmente. Cuando di esta presentación eran 19.

Es decir, hubo un aumento. Del mismo modo, en ese momento teníamos unas 10 fuentes de IP distintas y ahora estamos en alrededor de 100. Aquí vemos un gráfico que muestra las etiquetas de llave inesperadas. Otra vez, arriba a la derecha, vemos un aumento. Lo que yo considero es que todo esto viene del software Unbound. La línea azul se encuentra así como la vemos porque hay una población que está actualizando sus sistemas y que hizo lo que yo consideraría tonto porque agregaron la zona raíz ZSK al conjunto de anclaje de confianza, lo cual es inofensivo pero resultó en este pequeño aumento. Es un poco raro entender por qué pasó pero esto es lo que suponemos.

Mi conclusión entonces a partir de esto es que estos datos de señal tienen una buena calidad. No vi problemas ni nada que se le parezca. NAT y nombres que se forwardean a otros servidores, IP dinámicos que tienen visibilidad a dos de los servidores de raíz hacen que este análisis sea complicado. Para tener un mejor panorama, es mejor tener más servidores de raíz. Vamos a hablar un poco de eso más adelante.

Ya hablé sobre el 10 de octubre. Algo raro que ocurrió en ese día con los señaladores de los usuarios de Unbound. Quiero agradecerles a IFC por haber implementado y por haberlo puesto por default. También a otra empresa por entregarlo en Unbound. Quiero alentar a otros vendedores de software a que

también lo hagan. Este es el final de la presentación. No sé si vamos a tomar ahora las preguntas.

RUSS MUNDY: Sí, tenemos tiempo para un par de preguntas.

STEVEN BARRY: Soy Steven Barry, de .CA. Usted atribuyó parte de las varianzas y del aumento en las señales a las implementaciones en Unbound. Quizá yo no comprendí pero usted sabe que hay unos números relativos de Unbound versus las señales. ¿Usted sabe cuáles son esos números?

DUANE WESSELS: No tuve mucho tiempo de incluirlo pero en la charla de DNS hay algunas diapositivas que muestran cómo sabemos eso nosotros. La mejor manera de decirlo es que BIND da las señales que están disponibles 24 horas y Unbound… Yo los hice correr a ambos en casa. Unbound da los datos en intervalos más cortos y menos regulares. Esta es una de las razones por las cuales yo atribuí estas señales a Unbound. En cuanto al porcentaje, no sé el número exacto pero debe estar alrededor del 5-10%.

ONDREJ SURY: Gracias por la presentación. Nosotros acabamos de implementar esta característica ayer. Vamos a poder resolver esta funcionalidad pronto.

ROY ARENDS: ¿Usted sabe cuándo está programada la próxima implementación?

ONDREJ SURY: Honestamente no. Nosotros hicimos el código ayer. Todavía no hicimos la revisión. No podemos hablar de algo que no está testeado pero vamos a tratar de acelerarlo lo más que podamos. Voy a pedir a nuestros desarrolladores que lo hagan rápido.

ROY ARENDS: Yo sé que hablamos de esto ayer. Usted dice que los key tags, más allá del 4A5C y 4F66, además de estos key tags, ¿esto quiere decir que la señal tiene estas dos llaves y otra más? ¿Es correcto esto?

DUANE WESSELS: Sí, es correcto. Ese aumento a la derecha tiene las llaves esperadas más las inesperadas. Es decir, la línea azul indica los señaladores que muestran las llaves esperadas y las inesperadas. La línea roja, que está al final, marca solo los

valores inesperados de otras fuentes. Estos son otros experimentos.

RUSS MUNDY: Muy bien. Creo que tenemos que pasar a nuestra próxima presentación. Muchas gracias. El siguiente orador es Jaap Akkerhuis.

JAAP AKKERHUIS: Creo que esta diapositiva también muestra que la señal que una recibe es muy difícil de interpretar. Pueden ser claves que escapan los wildcars y otros. Vamos a hablar un poquito sobre Unbound, el 5011 y cómo implementamos cosas que no sabemos qué son. En general, si aparecen nuevas características en el DNS, nosotros tenemos la política de que somos conservadores. Es decir, básicamente cada vez que se inicia un borrador en Internet, si tenemos suficiente tiempo vamos a tener un llamado interno donde vamos a tratar de que se hagan algunas cosas y vamos a ir comentando sobre las nuevas características para ver si pueden funcionar.

Cuando la especificación es un poco más inestable, vamos a poder ir compilando la opción de runtime. La gente va a saber qué hacer y uno va a poder experimentar con eso pero tiene que hacer algún trabajo extra. Luego hay un periodo de 48 horas en

la RFC donde este borrador empieza a estar estable y solamente necesita de los comentarios. 48 horas puede requerir algunos meses en términos de la RFC pero vamos a tener en cuenta esta implementación como una opción de runtime. La gente que quiera vivir al límite puede activarlo, si saben lo que están haciendo.

Cuando el estándar es publicado como una RFC y pasaron las 48 horas, nosotros básicamente tomamos lo que se recomiende en ese RFC y lo ponemos como una configuración por defecto. Podría haber un cambio y no tendríamos que esperar a la siguiente implementación sino a la segunda porque hay una nueva característica y una nueva funcionalidad. Esta es la política estándar y algunos la utilizan y otros no.

¿Qué es lo que sucedió con 5011? El 5011 es un protocolo en Unbound por separado que se llama un anclaje de Unbound. La gente no toca mucho el código pero una vez que pasó el periodo de 48 horas nosotros pasamos a la base de código principal y lo que hicimos es incorporarlo en Unbound 1.4.0 en 2009. Incluso antes de que se implementara DNSSEC en la raíz. El problema es que este es un protocolo. 5011 es un protocolo y hay documentación donde le dice qué es lo que tiene que hacer sino solamente cómo hacerlo. Eso hace que el testeo sea muy difícil de hacer.

Durante años tuvimos lo que llamamos un uni test. Ese uni test permite testear distintas funcionalidades antes de publicar nada importante. Para la 5011, nosotros creamos este trabajo por defecto. Hicimos un test harness. Esto es lo que pasa cuando uno hace las diapositivas en el último momento. Hicimos un test harness en modo uni test y fingimos que las cosas pasaban más rápido en un periodo de tiempo de 30 días que se menciona en la 5011.

Este test harness fue hecho por .NIC y ellos lo hicieron un poco más genérico y lo implementaron como un software por separado. Después de 2009 hubo cambios incrementales porque se incorporaron arreglos de bugs pero nada esencial. Básicamente dimos soporte a la 5011 desde 2009, no más que eso.

Luego hicimos lo que se llaman bancos de prueba acelerada. Tuvimos el Rick-Roll, de Rick Lamb, el key rollover, que creo que se hacía cada 90 minutos, que es bastante rápido. Para hacer las pruebas tenemos dos equipos a quienes recurrir en Unbound para hacer un seguimiento de este protocolo falso. En realidad no es bueno esto porque significa un camino adicional que en realidad nunca se va a testear. Por los rápidos tiempos, tuvimos que acortar camino y cada vez que empezamos a hacer DNSSEC y 5011 en un periodo menor del periodo de 30 días requerido por el protocolo, no sabemos qué hacer. Para ser muy estricto,

Unbound siguió el protocolo a rajatabla. El rollover se anotó después del periodo de 30 días. BIND lo bloqueó y dijo: "Esto es rollover. Hagamos 60 días". Es una manera más avanzada de comprobar pero en este caso notábamos que esto pasaba y no era un caso especificado por ambos autores.

En el Unbound muchas personas, como [inaudible], de hecho están siguiendo el camino lógico. Quizá puedan estar haciéndonos 5011, que es otro problema quizá. Si hacemos DNSSEC en un momento anterior a los 30 días veremos que si estamos en esta situación desafortunada, lo único que hay que hacer es remover la etiqueta antigua, empezar el Unbound y todo va a funcionar bien. No es demasiado problema. La última versión de Unbound ahora ya reconoce esto.

Eso es lo que dije recién. Si tenemos este problema, sacamos la clave anterior y todo funciona bien. Después de algunos años vemos que nadie analizó la transición de este protocolo. Lo encontramos en la realidad pero la Internet, de todas formas, es un gran experimento. No lo vamos a remplazar por lo menos en breve por ninguna otra cosa.

RUSS MUNDY: Gracias, Jaap. Tenemos algunos minutos para preguntar a Jaap. No sé si hay alguna pregunta. No veo nada. ¿Hay algo en línea? Bueno, en ese caso, Jaap, muchas gracias. Luego tenemos a

Cristian Hesselman sobre el proyecto de historia, de Root Canary.

CRISTIAN HESSELMAN: Voy a hablar brevemente sobre el proyecto de Root Canary que es un esfuerzo conjunto de varias partes que vemos en la diapositiva. Yo pertenezco a SIDN Labs pero también están NLnet Labs, algunas universidades, además de la ICANN y RIPE. El proyecto del canario en la raíz también se conoce como el proyecto del canario en la mina de carbón virtual. Como saben, en el pasado los mineros llevaban un canario para indicarles si algo andaba mal. Con el contenido de monóxido de carbono en la mina, el canario moría. Cuando eso ocurría, sabían qué hacer. Lo mismo sucede con el traspaso de la KSK. Lo que queríamos hacer era rastrear el impacto operativo del traspaso y advertir, recibir señales de advertencia si algo andaba mal.

A la vez, mientras tanto, queríamos medir la validación durante el traspaso de la KSK desde una perspectiva global y básicamente aprender de este tipo de evento. Esas fueron las dos metas principales del proyecto. Es una metodología de medición la que estamos desarrollando aquí que utiliza distintas perspectivas. Las dos importantes son RIPE Atlas y Luminati. RIPE Atlas es el centro que quizá ustedes conocen, que tiene nodos de red en varios lugares del planeta, unos 9.000 lugares

que evalúan las redes de las personas en sus hogares básicamente. Luego la red Luminati es una red proxy que la gente usa para ocultar sus direcciones IP. Hablamos con APNIC para posiblemente usar sus mediciones e incorporarlas a nuestra metodología. Consideramos por último usar lo que se llama la perspectiva offline, hacer mediciones del tráfico a la raíz cuando se produzca el traspaso.

Esencialmente es un proyecto de medición. También en esta metodología firmamos varios dominios, tanto válidos como inválidos. Falsos o ficticios, por así llamarlos. Lo que queremos obtener de esta información es la cantidad de resolutores que se validan bien, aquellos que se validan incorrectamente y que producen SERVFAIL y los resolutores que no se validan. Como efecto secundario del proyecto estamos midiendo qué validadores soportan los distintos algoritmos. Esta es la red Luminati que es un servicio proxy de HTTP. Aquí lo importante es decir que da una perspectiva totalmente distinta de la que da RIPE Atlas, que cubre 15.000 sistemas autónomos pero 14.000 de estos no son cubiertos por RIPE Atlas. Hay gente que tiene antecedentes en red, la que maneja RIPE Atlas. No están en las redes de lo que llamaríamos consumidores regulares. Quizá sea más representativo del estado de las cosas en comparación con la red RIPE Atlas.

Hicimos un par de mediciones a 19 de septiembre, que es cuando aumentó la clave. No hubo nada especial. Son las SERVFAIL. No vemos demasiado cambio en este periodo. Perdón, tendría que haber dicho KSK. Es histórico, sí. Este es un gráfico similar que muestra el uso de TCP y UDP durante estos periodos. Supongamos que hubiera habido algo extraño. Los resolutores habrían conmutado TCP por el aumento del tamaño del mensaje. Fíjense que esto aquí no pasó. Estos son los bits de fragmentación. No hay demasiada fragmentación, como ven, tampoco. Todavía no pasó realmente nada porque se pospuso el traspaso de la KSK, lo que es bastante aburrido, pero bueno.

Queremos generalizar esta metodología que tenemos configurada para medir también los traspasos de clave a nivel de TLD. Lo queremos aplicar más genéricamente. También queremos medir y obtener más información de la forma en que los resolutores se comportan. Por ejemplo, en relación con los algoritmos de DNSSEC y también las implementaciones de los resolutores. Como decía, primero tenemos que manejar el traspaso. Si ustedes se dedican a mediciones de redes y tienen máquinas propias, desde ya agradecemos su colaboración en este proyecto corriendo un pequeño script que ayude a los resolutores a hacer queries de los dominios. Si a ustedes les interesa este proyecto, les agradecería que me contacten

después. Aquí tienen vínculos a más información sobre el proyecto del canario en la raíz. Esa era la última diapositiva.

RUSS MUNDY: Gracias, Cristian. Un aplauso para Cristian. Voy a asegurarme de que todos estén despiertos y por eso cambié el orden. ¿Hay alguna pregunta para el proyecto?

ROY ARENDS: Hola, Cristian. Soy Roy Arends. No sé si lo oí bien pero creo que usted dijo que hay una nueva KSK el 19 de septiembre. Ustedes miden el aumento…

CRISTIAN HESSELMAN: Sí, el aumento de mensajes.

ROY ARENDS: Es cuando se hace el traspaso de la clave del mantenedor de la zona raíz. Se hace cada tres años, ¿no?

CRISTIAN HESSELMAN: Sí. Lo dije mal.

ORADOR DESCONOCIDO: Yo soy [inaudible]. Hola, Cristian. ¿Tienen datos por país acerca de cómo los algoritmos soportan algo alternativo a lo que decía Geoff?

CRISTIAN HESSELMAN: Tenemos mucho material. No lo incluí en estas diapositivas pero lo encontrará en el sitio web del proyecto que es rootcanary.org.

ORADOR DESCONOCIDO: Gracias.

JAAP AKKERHUIS: De hecho, usted puede ver cómo se hacen las mediciones en tiempo real.

ORADOR DESCONOCIDO: Vi muchas mediciones. ¿Estas mediciones también incluyen los datos de la Luminati?

CRISTIAN HESSELMAN: La verdad es que no lo sé. Lo tengo que verificar.

JAAP AKKERHUIS: Tengo varias consultas. Necesitamos representantes del RIPE Atlas en esta zona. Si me pueden contactar, aquí les explico.

RUSS MUNDY: Muchas gracias. El siguiente presentador es Geoff Huston. Le paso la palabra a Geoff.

GEOFF HUSTON: Buenos días a todos. Esa no es la diapositiva. Ese es usted. Ese no soy yo. Yo no soy Roy. Hace tiempo que no veo estas diapositivas. A lo mejor están desactualizadas. Tenemos que recortar un poquito el tamaño. Me parece que no sería problema. Un poquito a la izquierda. La cuestión global para la ICANN en el manejo del traspaso de la KSK, el problema real es cuántos usuarios están en situación de riesgo. Sabemos bastante bien que en este momento el 25% de los usuarios hacen validación de DNSSEC. No resolverán un nombre si es inválido. En otras palabras, no tiene un registro de resolutores no validados. Es un gran número de usuarios. Podría verse afectado potencialmente por el traspaso de la KSK si es que de una u otra manera sale mal. Ese es el límite superior. Eso es lo que pudimos medir.

En este lanzamiento hay dos elementos de riesgo. El primer elemento es cuando una respuesta relativamente grande es una parte integral de la incorporación de un resolutor, porque en este momento la respuesta más grande que hemos tenido en esta fase es de 1.414 octetos. La buena noticia es que son menos

de 1.500, que es el estándar de facto para UDP. La mala noticia es que si nos preguntamos por qué 1.280, la repuesta es que es 1.024 + 256. ¿Qué significa? Nada. Este número, de todas formas, es más que 1.280. Es una gran cantidad de usuarios. Hay una cuestión de fragmentación que en este momento entra en juego.

La segunda cuestión. La RFC 5011 nos dice que no podemos testear producción, que podemos testear entornos, por así decir, de juego pero no lo vamos a saber hasta que testeemos el entorno real. No hay manera de testear el entorno de producción. Si fracasamos, fracasamos muy mal. Si no se tiene un caso de confianza, no se puede hacer nada. Es una pérdida de servicio. El resolutor directamente va a dejar de brindar servicio. Si el usuario pasa una query a estos resolutores afectados hay potencial de que se caiga el servicio. Nosotros hasta ahora hemos oído hablar de que hay que medir los resolutores. Esa es la pregunta. Lo que oímos, son resolutores. ¿Cómo funcionan? Los resolutores soportan mecanismos de señal enviando una señal. Duane explicó esto.

Entremos en un poquito más de detalle. Solo los servidores raíz pueden ver esa señal y resolutores recursivos de reenvío. Nadie más que estos. Es como una señal que no diría que es secreta pero es difícil de encontrar a menos que se corra un servidor raíz y se busque. En segundo lugar, es un query sin atribución. Si usted es mi forwarder, pareciera que usted está reportando, no

yo. Ahora yo soy invisible. Todos estos resolutores que utilizan forwarders son visibles y eso confunde la atribución de la señal. Ustedes saben que una señal es una señal pero en el mundo de DNS algunos resolutores son mucho más importantes que otros. Los Google, los servidores del DNS público de Google brindan DNS para un gran porcentaje de la población y sus resolutores son muy importantes.

Mi resolutor en casa me da las respuestas en mi lugar. Yo no diría que esto esté mal. A mí me gusta pero al resto de ustedes no le importa, ni tiene por qué importarle. Tratar de entender que algunas señales son muy importantes y otras no por el número de usuarios no resulta evidente según los datos. Algo que tampoco es claro es si un resolutor falla, la mayoría de estos tienen múltiples subresolutores. Si vas de A a B, puede que recibas respuesta de B, así que no está tan mal. Los usuarios van a encontrar.

Toda esta cuestión de medir los resolutores como un fin en sí mismo no resulta útil para responder esta pregunta. Respuesta incorrecta. Lo que hay que saber es cómo responder la siguiente pregunta. ¿Qué clase de query revelaría el estado de las claves confiables en los resolutores? Puedo anticipar ser víctima de servicio. Todos mis resolutores que dependen en este momento, ¿se van a caer o alguno va a seguir funcionando? ¿Podemos dividir esta query que nos revele esta situación? No, no

podemos. Alguien me puede decir: “Geoff, te equivocas. Hay una manera adecuada de hacerlo”, pero hasta ahora la gente sigue preguntándose y algo tiene que cambiar.

Hay algo que se puede incorporar o hay que cambiar el comportamiento de los resolutores. Tenemos que hacer algo. Si pudiéramos cambiar el comportamiento de los resolutores, ustedes pueden decir: “No lo hicimos”, pero sí lo hicimos, a través de un RFC. Hemos visto que algunos resolutores están dispuestos a cambiar el código esta es la esencia de la idea. ¿Puedo poner una etiqueta mágica que no es el nombre principal, solo una etiqueta? Si ustedes ven esta etiqueta en un nombre de dominio y ustedes son resolutores de validación, a lo mejor les conviene cambiar Good (bueno) por Bad (malo) en la respuesta si esta está añadida al not tag key, es un fallo por falta de confianza de la clave. La diferencia entre los resolutores que soportan este mecanismo y aquellos que no lo soportan se hace a través de la inversión lógica, si no es una clave confiada.

Ustedes pueden hacer este query al igual que cualquier otra persona, incluso como usuario: label.some.signeddomain. También porque es importante pueden generar una etiqueta que esté firmada mal a propósito. Es fácil generar una etiqueta mal firmada. Si miran el tipo de respuesta, hay cuatro tipos de resolutores, de comportamiento de resolutores que les interesan, los que soportan el nuevo mecanismo y que cargan el

nuevo KSK. Vamos a tener un registro para la primera query y lo mismo para la segunda y la tercera. El resolutor soporta el mecanismo pero no cargó la clave. Luego hay un switch over. Piensan abrir nuevos casos.

Si el resolutor no aprendió sobre este nuevo mecanismo va a tener un patrón distinto. A record. Si el resolutor no está validado, vamos a tener de nuevo los A record. Pueden distinguir los cuatro casos que a mí me interesan pero no hay una sola resolución. Suele haber varias y suele haber forwarders. La situación es más compleja. El análisis de los resultados es bastante similar. Si tomo todos los resolutores recursivos y tomo todas las respuestas, ahí va a estar todo bien. Supongamos que hay algunos archivos que dicen que ustedes están bien y otros que no. Los otros dos tipos de respuestas dicen: “En todos los resolutores que ustedes utilizan, algunos no soportan este mecanismo y no pueden decir cuál va a ser la respuesta”. Esos son los dos resultados donde no tenemos un conocimiento. Después puede haber uno de los resolutores donde no valida.

Pónganlo entonces en una página web. Háganlo ustedes mismos. Testéenlo. O si conocen una campaña online, y yo conozco, pueden poner el archivo en javascript o HTML y miren la cantidad de millones de usuarios porque esa medición puede mostrar no solamente el estado del key roll sino también del update del mecanismo en sí por usuario. Es decir, es muy posible

en una campaña publicitaria online no solamente ver que esto se implemente sino cuáles son los casos confiables. Estamos jugando con el DNS. Es necesario pensar en la privacidad y la seguridad. Esto no revela la identidad de los usuarios finales. Son solamente resolutores no usuarios y no contienen ninguna información de identificación. Lo que ustedes hacen les importa a ustedes pero no tienen que identificar a los usuarios. Nunca cambien de seguro a inseguro. Es una mala idea. Lo único que hace es cambiarlo autenticado a inseguro y muchas veces depende del estado de la llave confiable cuando estos resolutores tienen ciertas etiquetas.

No es algo exclusivo que pueden hacer los servidores de raíz. Ustedes así van a poder tener los datos. Los resultados vuelven a ustedes como respuesta a estas query de DNS. Es una forma más democrática de testearlo y de ser un poco más abiertos. Los ISP se pueden testear a sí mismo o los ISP pueden testear a otros ISP, depende de ustedes. Hay un borrador ahí, como suele ocurrir. Tiene unas dos semanas. Si ustedes se ocupan del DNS, y les agradezco el feedback que me puedan mandar, nosotros estamos muy interesados en los comentarios que puedan ustedes tener. Cuando ustedes toman la señal de la RFC 8145 en términos de atribución y de entender la importancia de esa señal versus la cantidad de usuarios, este es un enfoque distinto que mira las llaves confiables para usuarios y para el entorno

holístico del DNS en sí. No va a revelar la capacidad de un resolutor individual en general porque el DNS no es así. Sí va a revelar si el usuario está en un buen o mal lugar en cuanto al key roll. Creo que me quedan unos 46 segundos para las preguntas. Ya me quedé sin tiempo.

ROBERT MARTIN-LEGENE: Hola. Soy Robert Martin-Legene, de PCH. Siempre me gustan sus presentaciones. ¿Usted consideró tener en cuenta EDNS 0 para los queries, si es que queremos tener en cuenta el forwarder? Algo que podría haberse detectado si se le enviaba al usuario final. Quizá podemos poner una opción de EDNS que permita el forward.

GEOFF HUSTON: Yo doy vuelta a este argumento y no tiene nada que ver con el query. Tiene que ver con la respuesta. Esa es la parte esencial. No hay casi información que venga al servidor de nombre autorizado. El caching no importa, el forwarding tampoco importa. Este es uno de los patrones de las tres query. Las respuestas que les vienen a ustedes son las que son importantes. Los servidores de nombre autorizado son ignorantes. Es decir, no conocen a los resolutores que ustedes tienen. Solamente ustedes los conocen y este test es para ustedes, no para ellos. Aquí, en la oficina del CTO, cuando están tomando en cuenta el

key roll, ellos están pensando lo que van a decir en el diario. Ese es un problema de usuario, no de resolutor. Por eso yo quiero volver al resolutor y las respuestas entonces son las que son importantes, no las consultas o queries.

ROBERT MARTIN-LEGENE: Internet no solo es usuarios. Hoy hay muchos sistemas automatizados. Si algo deja de funcionar y la gente no se da cuenta durante dos meses, eso es algo que puede muy bien suceder porque muchos sistemas automatizados no muestran ningún tipo de error automatizado. Mi mamá llama a alguien si la computadora no funciona. Ella no se muere porque no funcione Internet. Eso es algo que hay que medir.

GEOFF HUSTON: Esto es susceptible a una gran cantidad de queries con una campaña publicitaria. Si lo hacemos bien, podemos hacer muchas muestras. No vamos a testear a todos los usuarios. No vamos a testear a todos los dispositivos porque eso no se puede hacer pero con los mismos mecanismos que nos muestran 11% o 12% de los usuarios que usan solamente validación de DNSSEC, podemos tener la respuesta y el mismo nivel de confianza respecto de si va a funcionar un roll de KSK.

ROY ARENDS: Quisiera también decir que los sistemas automatizados también pueden utilizar esta técnica. Están todos armados por personas.

RUSS MUNDY: Creo que tenemos que avanzar. Vamos a dar a Roy suficiente tiempo para cubrir su presentación y para que haya preguntas y respuestas sobre el estado de la implementación del KSK.

ROY ARENDS: Esta es la séptima vez que doy esta presentación así que quisiera que levanten la mano quienes no vieron esta presentación todavía. Bueno, con esto me alcanza. Mi nombre es Roy Arends. Trabajo en la oficina del CTO. Soy investigador. Si hacen ustedes validación de DNSSEC necesita una llave pública. Este anclaje de confianza que es para siempre y hay que renovarlos. En DNSSEC lo llamamos traspasar o cambiar la llave. Ya mencionamos que no hay formas de confirmar esto. Cuando lo diseñamos hace algunos años, el equipo creó planes. Hablamos con los vendedores, con los gobiernos, etc. y el 11 de octubre de 2017, que fue una fecha importante, nosotros no sabíamos quién estaba validando o quién tenía la configuración correcta.

El 11 de julio de 2017 introdujimos el nuevo KSK y monitoreamos si hay cambios fundamentales en el tráfico del servidor de raíz. Mi amigo Duane trabaja en Verisign y él tuvo acceso al tráfico de

ruta. En la raíz B, D, F y L. Eventualmente, logramos que todos los servidores de raíz nos den servicio, lo que no es más que ver el tamaño de respuesta del DNSKEY. Hace un par de años, Geoff y yo hicimos una investigación sobre el traspaso. Los resolutores siguen buscando la llave de DNS pero no ocurrió nada. Tenemos excelentes estadísticas con un gráfico muy lindo de lo que ocurrió el 11 de julio.

Luego, un mes después, no hay nada que ver respecto del tráfico. El 19 de septiembre, eso es lo que yo mencionaba antes. Nuestro socio de Verisign introdujo un nuevo esquema ZSK. Lo han estado haciendo desde el año 2010. La única excepción aquí es que esta es la primera vez que aumenta el tamaño de la respuesta. Seguramente ya vieron esta diapositiva en la presentación anterior. No teníamos antes conocimiento de cuál es el anclaje de confianza. Ya hablamos del RFC 8145, del BIND9, así que esto lo voy a saltear.

Acabo de escuchar de [André Phillippe] que dijo que en el futuro cercano vamos a tener una versión que va a estar funcionando. No sé si el recursor de Microsoft también lo va a usar. Hay unos 4 millones de direcciones únicas que utilizan estos resolutores que están en el servidor raíz. Olvídense en realidad de ese número. Es mucho más alto si ustedes combinan todos los servidores raíz y si hacen un estudio sobre las direcciones únicas. 4.2 millones es

el lower bound. Los números que tuvimos con la RFC 8145 son bastante bajos.

Disculpen. Las estadísticas son desde el 24 de octubre hasta el 1 de septiembre. Tenemos unos 27.000 de esos 4.2 millones. El número total que reporta los KSK es 1.631, es decir, el 6%. Yo no miré si estos resolutores están validados. Podría ser que sí lo estén. Alguien tiene que chequear esta quita que está funcionando. Si ustedes lo hacen, seguramente va a bajar un poco el número pero no tanto.

Mis colegas ya dijeron que este análisis es muy complicado. A mí, en general, me gusta la propuesta de Geoff que me hizo hace dos años. Antes de que diga algo mal, esta es una opinión personal. No estoy hablando en representación de ICANN pero me gusta la propuesta. Sabemos por qué el KSK de 2010 está reportado y no el de 2017. La última versión de BIND reporta el anclaje de confianza, a pesar de que no están validadas, lo cual es un poco molesto porque ahora tenemos una señal falsa. La llave está configurada y seguramente no está validando.

Antes de la 5011, había una configuración donde uno pone toda la confianza, lo cual tiene sentido, pero después de 5011 necesitábamos una configuración diferente para estar seguros de que algunas claves se pueden actualizar con 5011 y que se configuran manualmente. BIND utiliza managed keys para

configurar el 5011. Esto lo voy a saltear. Hay muchas cuestiones que reportar. Vamos otra vez al plan y al proceso. No hay nada aquí que esté sucediendo. Esto fue antes de la reunión del DNS. Tuvimos un informe de Verisign. Allí pusimos nuestros propios datos. Nosotros no podemos decidir las cosas ad hoc por eso consultamos el plan operativo. Este es el plan que tiene ya unos años. La comunidad lo ratificó. Dice que los socios de management de la zona raíz podrían también decidir extender cualquier fase para tiempo adicional. Por ejemplo, si hay nueva información que indica que la próxima fase pueda llevar a complicaciones, la fase actual deberá ser prolongada y esto se refiere a un escenario extendido.

El 27 de septiembre se extendió este escenario. Escuché algunos informes de que algunas listas de correo tuvieron esta información antes que otras pero esto se debe a que nuestros equipos de comunicación no están en las listas de DNSSEC y tuvimos que reenviar esa información muy rápido. Como dije antes, no sabemos cómo estos representantes informan a estos validadores. Geoff ya dijo que estos validadores no son lo mismo que los usuarios finales. Yo estoy tratando de trabajar con Geoff para compartir datos. Vamos a mostrarles los números que reportan estos key tags para ver si tiene algún sentido. La cantidad de usuarios también que hay. Creo que estamos

hablando de 750 millones que están validando. Ese es el número que escuchamos el otro día.

La mitigación es difícil. Ya tuvimos una campaña multianual para comunicarnos con los operadores. Estos problemas son específicos de la implementación, que hacen que el problema no sea más fácil. Nosotros ya sufrimos esto en el pasado y, como dijo Geoff antes, solo podemos hacerlo operativamente y no lo podemos testear en un entorno. Pusimos entonces la implementación hasta tener más información y entender mejor la situación. Va a ser al menos un trimestre.

Para aquellos que tienen preguntas sobre esto, esto implica uno o más trimestres. Siempre estamos alineados con el trimestre y la razón de las ceremonias de la llave es que ICANN las organiza cada tres meses y no vamos a poder determinar cuántos trimestres demorar. Vamos a contratar a una empresa para ir rastreando los 500 resolutores en base a las direcciones IP y entender por qué está ocurriendo esta configuración equivocada por defecto. La recolección de datos continúa.

Quiero decir una cosa sobre Unbound. Duane dijo que Unbound fue implementado el 10 u 11 de octubre. Lo que ocurrió es que el 10 de octubre es tan bien el último día en que se utilizó el [ZSK-Q3] y que se agregó a la señal. El hecho de que Unbound esté

enviando ese query no significa en realidad que Unbound esté validado. Podría ser un resolutor.

JAAP AKKERHUIS: No, no, no. Solamente da una señal cuando está validando.

ROY ARENDS: Si yo le hago una consulta a Unbound que utiliza una key tag, ¿eso va a ir a la raíz y se lo va a preguntar? ¿Va a resolver la key tag?

JAAP AKKERHUIS: Bueno, depende de cómo vamos a configurar el DNS. Si el usuario tiene forwarders, la gente hace cosas muy raras. Pone forwarders…

ROY ARENDS: Disculpe, está tomando mi tiempo. Les voy a mostrar unos datos después. Quería que entendiera que Unbound no es siempre un problema. Lo último que quería decir de esta parte es que no pasemos al KSK 2017. No lo retiremos. Hay gente que dice que hay que remover KSK 2017 de la configuración pero no lo hagan. No lo hagan. Tengo otra serie de diapositivas que son sobre la frecuencia del lanzamiento de la KSK. Era para los expertos pero me quedan unos minutitos. Voy a aprovechar. Muy rápido. Es

una breve discusión sobre la frecuencia de lanzamiento de la KSK.

Comenzamos a usar la clave antigua en 2010. Planeamos usar la nueva KSK en 2018, si no pasa nada más. Hay quienes son muy intensos a la hora de defender la configuración manual del nuevo anclaje de confianza y hay otros que no. Los validadores pueden tener algunos problemas de configuración que pueden tener particiones de read only, de lectura solamente, o usan configuraciones incorrectas. Hay bugs.

Hay dos escuelas de pensamiento. Hacer un lanzamiento frecuente. Esto no significa a menudo. Frecuentemente significa a intervalos fijos. Significa, si no se rompió, no pasó nada, para qué hacer el lanzamiento. La comunidad técnica del DNS hace algunos años estuvo con la postura de hacer el lanzamiento frecuente. Yo decidí poner aquí lo que sería un límite de frecuencia que es un límite inferior de frecuencia. La frecuencia superior es sencilla. Por ahora diríamos cinco años. El límite inferior absoluto es tres meses por las ceremonias de cambio de la clave. Si lo cambiamos más a menudo que tres meses, sé que es ridículo pero hay gente que dice que lo cambia todas las semanas, por eso lo puse aquí. El límite inferior de mayor frecuencia es tres meses. Cualquier cosa por encima de esto requiere muchísimo trabajo.

¿Cuál es el efecto de lanzarlo cada tres meses? Tenemos tres etapas en la introducción de la clave. Si lo hacemos cada tres meses, colapsamos tres estados en una sola instancia. Introducimos la clave C, comenzamos a firmar con la clave B y revocamos la clave A. Este es un gran problema pero el tamaño de respuesta mínimo es 1.986 bytes, que es imposible. Además, despliegues manuales o semiautomáticos tienen que actualizarse cada tres meses. Yo lo pongo aquí. No es una opinión. Es lo que ocurre. Si lo hacemos cada seis meses, no presenta problemas en cuanto al tamaño de la respuesta porque no hay que hacer un colapsado completo. Se siguen colapsando dos etapas en una sola. Se introduce una nueva key, se revoca la vieja llave y se usa la nueva. La primera es la introducción y la segunda es revocar la clave antigua y usar la nueva. Esto presenta un problema. Si hay un colapsado de estas dos etapas en una sola, no se puede volver atrás. Hay que rediseñar todo el proceso.

Si se hace el lanzamiento cada nueve meses, no tenemos problema de tamaño, podemos usar el diseño del plan actual, la mayor frecuencia no significa cambios fundamentales del diseño. Sé que hay diferencias de opiniones en la comunidad de operaciones pero esta es nuestra perspectiva.

Cada año el espacio de tiempo se mueve un trimestre. Cada cuatro años, lo tendremos dos veces en un año. No es la

situación óptima para los operadores por la falta de previsibilidad que esto puede implicar. Mientras que el lanzamiento cada año tampoco tiene problemas de tamaño. Se puede usar el diseño del plan. Además, es más predecible. Todas son cosas buenas. Es levemente mejor para los operadores. Más de un año no hay diferencia significativa con hacerlo cada año. Es más o menos lo mismo si se hace cada año o cada fin de año. Yo imagino que si se hace con frecuencia, que no es lo mismo que a menudo o seguido, está bien pero no más rápido de un año y un límite máximo de cinco años.

Ayer hablé con Jaap y no quiero quitarle la pregunta pero Jaap tuvo muy buenos comentarios. Él me preguntó: "¿Deberíamos hacer un lanzamiento antes de tomar una decisión?" Tiene razón. Prometí hacer esta presentación. Podemos seguir hablando pero sí, es un poco prematuro porque no hemos hecho todavía el cambio. Gracias.

RUSS MUNDY: Gracias, Roy.

DUANE WESSELS: ¿Podemos volver a la diapositiva de los seis meses? ¿Me puede aclarar? Usted dijo que no hay manera de volver atrás, de hacer

una reversión del lanzamiento. ¿Roll back y extender sería lo mismo en este caso?

ROY ARENDS: No. No es lo mismo. Si se revoca la clave antigua en el momento en que se usa la nueva, no se puede volver atrás pero si se demora el lanzamiento de la clave, se puede utilizar la antigua durante un trimestre.

DUANE WESSELS: Estoy pensando en la situación actual en que extendimos el periodo previo publicado, que lo extendimos y no pasamos al siguiente. Quizá es difícil en este momento definir esto. Quizá debamos hablar en persona.

RUSS MUNDY: Hablamos de algunas cosas muy importantes. Como nuestro grupo está asociado al SSAC, el SSAC63 se ocupó de muchas de estas cosas hace unos años y una cosa importante en ese momento es aprender lo más posible de este lanzamiento para aprender para los futuros. ¿Tenemos alguna otra pregunta rápida para Roy antes de ir al almuerzo? Robert.

ROBERT MARTIN-LEGENE: Robert Martin, de PCH. Algo que podemos considerar a la hora de definir qué funciona y qué no funciona, van a pensar que estoy loco, es que los servidores raíz podrían proveer datos firmados con la clave antigua y los otros firmados con la clave nueva. Entonces, no habrá una denegación de servicio para el usuario pero va a haber un cuestionamiento de quién estaba usando cada clave.

ROY ARENDS: Esta idea no es mala de por sí. Se mencionó varias veces. La idea es tener una serie de servidores en la zona raíz con la clave actual y la anterior y observar la progresión natural de ambos anclajes de confianza validados pero eso es increíblemente difícil de medir. De hecho, no ayuda porque lo que uno quiere es que en algún momento todos pasen a la KSK 2017. La pregunta es cuándo hacemos el switch off. No ayuda, no brinda información nueva. Nosotros ya sabemos quiénes son. Asumiendo que este sea un muestreo apropiado, aquí están. Mi instinto me dice que no.

ROBERT MARTIN-LEGENE: Yo no digo que deba hacerse pero podría hacerse. Entiendo muy bien por qué no sería el curso a seguir.

ROY ARENDS: Hay muchas cosas que podrían hacerse y que no debemos hacer.

RUSS MUNDY: Vamos a agradecer a Roy por su presentación. Por haberla ofrecido por séptima vez. Ahora Jacques.

JULIE HEDLUND: Fue al baño y ahora vuelve.

RUSS MUNDY: Tenemos el cuestionario del DNS.

JULIE HEDLUND: Tenemos tiempo porque el almuerzo es recién a las 12:15. Tenemos tiempo.

GEOFF HUSTON: La razón por la cual la respuesta es negativa claramente es porque cuando hay dos claves listadas en los registros de recursos firmados por la clave vieja, esto implícitamente indica la confianza en materiales firmados con la clave nueva porque se confiaba en la clave antigua. Si pasamos a un servidor de raíz distinto, como teníamos la antigua en la caché, confiamos en la nueva con el servidor modificado, porque confiábamos en la clave antigua y la clave nueva está firmada con la clave vieja.

Toda esta cuestión se complica por el hecho de que clave nueva firmada con clave vieja se confía por esa transición. Tenemos que separar dentro de la raíz con nombres de dominio distintivos que tienen distintos comportamientos de DNSSEC. “Este es un nombre que solo podemos validar con la clave nueva, si está en el trustor”.

Hay que trabajar en la raíz, en el protocolo de validación y en el resolutor. Por eso es tan difícil y no estoy seguro de que los datos sean de utilidad porque, como decía al comenzar, no son los resolutores los que nos deben preocupar sino los daños que podríamos hacerle a los usuarios. Es necesario alejarse de los resolutores y refocalizarse en los usuarios. Ya tenemos a Jacques en la sala.

JACQUES LATOUR: ¿Alguna otra pregunta? No entiendo cómo me convertí en el maestro de los cuestionarios. No sé si alguien más abandonó ese cargo. Bienvenidos al gran cuestionario de DNS y DNSSEC para ICANN 60. Frente a ustedes tienen el cuestionario con 10 preguntas que responder. Tienen la planilla. Si no la tienen, pueden acercarse a la mesa y retirar una. Me imagino que todos tienen con qué escribir. Aquí están las reglas que me enseñó Roy. Tengo razón. Me puedo equivocar pero no importa. Tengo razón. Por eso soy el maestro del cuestionario autoritativo. Hay una

sola respuesta correcta por pregunta. Es un punto por respuesta correcta. Es muy simple. Son 10 preguntas y un máximo de 10 puntos. No hay manera de sacarse un -17. Nada por el estilo.

JACQUES LATOUR: Comencemos. Pregunta 1: ¿Cuál fue la fecha en que se suponía que se iba a hacer el traspaso de la clave para la firma de la llave de la zona raíz? A) 11 de octubre de 2014. B) 11 de octubre de 2015. C) 11 de octubre de 2016. D) 11 de octubre de 2017. E) Iba a pasar el año pasado pero decidimos no hacerlo.

Tres, dos, uno, cero.

Pregunta 2: ¿Qué feed de Twitter rastrea los cambios de la zona raíz? @therootchange, @changeroot, @difroot, @root, @IamGroot.

Siguiente. Pregunta 3: ¿Qué lista de correo permite ver mejor y reportar los problemas con la DNS en general? DNSoperation@list.DNS-OARC, IamGroot@list.DNS.DNS-OARC, DNSSECcord@elist.ISOC.org, DNSop@ietf.org o helpwithdns@icann.org. Recuerden que siempre tengo razón. La que crea que es la respuesta correcta, lo es.

Pregunta 4: En draft IETF homenet.14, ¿cuál es el dominio designado para uso no exclusivo en redes residenciales, hogareños y designa este dominio como dominio de uso

especial? A) .HOME. B) Arpa/home. C) .HOME.[MAISON.CASA.MEZO]. Creo que es chino. Home.ARPA o .MAISON.

Pregunta 5: ¿Cuál fue el ccTLD que se firmó con DS en la raíz más recientemente? A) .AX (Islas Aland). B) .GW (Guinea-Bissau). C) .BM (Bermudas). D) .SA (Arabia Saudí). El que se firmó más recientemente. Lo mencionamos hoy por la mañana.

Esta es especial. Empieza con: Perdón porque soy canadiense. Dice: ¿Cuál de las siguientes afirmaciones describe mejor la autenticación basada en DNS de entidades de nombre, el valor dos de los usos de certificado? A) No asignado. Qué difícil para los intérpretes esto. B) [PKXDA-CA]. C) DANE-TA. D) DANE-EE. E) PKIX-EE. Esto es tan obvio.

La que sigue. Pregunta 7: ¿Cuál es el porcentaje de la totalidad de TLD firmados en la raíz con delegación segura en la raíz? Esto lo dije hoy temprano, cuando todos dormían y yo dije que era importante.

Esta me gusta. ¿Cuál de estos dos papers de Paul Mockapetris publicado en noviembre de 1983 marcó el comienzo del DNS? ¿Qué dos papers? A) BCP16 y BCP17. B) BCP42 y BCP78. C) RFC882 y RFC883. D) RFC1034 y RFC1035.

Pregunta 9: ¿Cuál es un método de direccionamiento y enrutamiento de de redes en el cual los datagramas de un único remitente son enrutados a cualquier nodo o nodos de destino seleccionados sobre la base de cuál es la ruta más próxima de menor costo, más saludable o menos congestionada, o alguna otra medición de distancia? Multicast, Anycast, Unicast, Star Trek Subspacecast o [Flurrycast].

¿Qué significa DNS? Servidores de nombres de dominio, Sistema de nombres de dominio, Software de nombres de dominio, Servicio de nombres de dominio o Espacio de nombres de dominio. Esta pregunta la puse porque yo no sé cuál es la respuesta. Es cuestión de elegir una, que será la correcta. Seguramente vamos a hablar de esto durante el almuerzo. Es el momento de corregir. Entreguen la hoja al vecino. Es muy fácil. Es una respuesta por pregunta. Un punto por respuesta. Máximo de 10 puntos. Vamos a ver si nos equivocamos.

Pregunta 1: La respuesta es la D. Tenía que tener lugar el 11 de octubre de 2017. ¿Lo hicieron bien? Tienen que sacar por lo menos un punto para ir a almorzar. Esa es la regla del auspiciante. Si sacaron cero, no almuerzan.

Pregunta 2: La respuesta es @difroot. Me gustó @IamGroot.

Pregunta 3: A. DNS operation list es el mejor lugar si ustedes tienen problemas del DNS. Si no están en esa lista, pueden ir a buscarlo en Google y ser parte de eso. Es un buen recurso.

Pregunta 4: La respuesta es la D. Me gusta la C. Deberíamos tener este dominio enorme con todos los idiomas.

Pregunta 5: .GW (Guinea-Bissau) se agregó en octubre de 2017. Esa fue la última adición.

Pregunta 6: La respuesta es la C. Trust anchor assertion es la respuesta correcta.

Pregunta 7: El número es 90% de los TLD están firmados.

Pregunta 8: Esta fue nuestra RFC882 y 883. ¿Hay alguna relación entre la 883 y el año 83?

Pregunta 9: Anycast. La próxima versión es Subspacecasting. Tenemos que empezar a trabajar en esa versión. [Flurrycast] es lo que mandamos a todos lados y todos responden.

Pregunta 10: No sé muy bien cuál es la respuesta así que elegí la B. Vamos a ver quién es el gran gurú del DNS. Levanten la mano si tienen cinco o más. Seis o más. Siete o más. Ocho o más. Nueve o más. Y 10. Estamos en presencia de un gran gurú del DNS. Deberíamos darte una estrella.

RUSS MUNDY: Sin duda se ganó un almuerzo gratis.

JACQUES LATOUR: 9 de 10. Muy bien.

ORADOR DESCONOCIDO: El almuerzo es en el hall 4. Tienen que pasar registración, doblar a la derecha. No tienen que pasar por el detector de metales. Simplemente entren a la derecha y recuerden que tienen que tener su ticket.

[FIN DE LA TRANSCRIPCIÓN]