ABU DABI – Taller sobre el DNSSEC – Parte 3
Miércoles, 1 de noviembre de 2017 – 13:30 a 15:00 GST
ICANN60 | Abu Dabi, Emiratos Árabes Unidos

JACQUES LATOUR: Vamos a tener que esperar algunos minutos antes de conseguir que la demostración funcione.

Bienvenidos al taller de DNSSEC parte III. El próximo orador es Wes Hardaker, que va a hacer una presentación LocalRoot. Sírvase usted mismo.

WES HARDAKER: Por curiosidad, ¿cuántos de ustedes administran un resolutor recursivo en sus infraestructuras? ¿Cuántos de ustedes administran cualquier resolutor? Nos podrían contar qué hacer. Hoy voy a hablar… ¿Podemos ponerlo en pantalla completa? ¿Perdimos el documento? ¿Cuántos de ustedes conocen el RFC 7706 que sirve a la zona raíz en la dirección de loop back? Bueno, hay algunos. La parte importante es que nos permite servir la zona raíz a través de las redes locales que usan resolutores recursivos sin tener que hablar con la zona raíz. De eso vamos a hablar. Tenemos un proyecto que se llama LocalRoot. Les voy a contar lo que significa.

En primer lugar, ¿qué es LocalRoot? Como decía, es un proyecto para permitir cargar la zona raíz en los resolutores locales. Como un breve antecedente, esta es la resolución clásica del DNS. De un lado tenemos una lista de clientes que todos intentan hacer lookups en el DNS, ya sea una página web o el teléfono, actualizaciones automáticas, hablan con un ISP. Puede ser la red inalámbrica aquí. En el ISP hay un resolutor recursivo cuya función es responder todas las queries que el cliente envía. Lo hace hablando con el resto de la infraestructura del DNS. Por ejemplo, a la derecha vemos que está la zona raíz, .COM y .ORG. Debajo tenemos ejemplos como example.com y a la derecha icann.org.

En este ejemplo clásico supongamos que el cliente dice que quiere ir a www.example.com, el resolutor en el medio envía la pregunta y se la envía a la raíz. www.example.com va primero a la raíz y la raíz es responsable de dar la siguiente iteración a dónde ir. En este caso, está .COM. Hay que preguntarle a él. El resolutor le pregunta a www.example.com y .COM da ejemplo al resolutor.

En este concepto hay una caché en el resolutor que recuerda cosas. Recuerda que existe .COM y recuerda que existe example.com. Eso no sirve para cuando el siguiente cliente pregunta por icann.org, porque .ORG no está en la caché ni icann.org. Tienen que empezar el proceso de vuelta. La verdad

es que no soy un fan de Adobe Connect. ¿Dónde estoy? En este caso, por ejemplo, todos los clientes preguntan dónde está www.exam.com. Como el resolutor ya conocía el .COM, no tenía que ir a preguntar dónde estaba .COM. La conexión baja desde .COM. Fíjense que hay muchas menos flechas en la pantalla, que ya tenía .COM en la caché.

Esto es lo que yo propongo cambiar con mi proyecto. Loguear todo en el resolutor. ¿Qué pasa si en lugar de que la resolución se haga donde el resolutor contiene solo la información de nivel superior de la raíz, yo te doy toda la información de la raíz? Es decir, hacer una caché de todos los TLD que existen: .COM, .ORG, .CX para los países, .HORSES, que es uno de los gTLD y hacer una pseudocaché con toda la información en la raíz. Esto lo que significa es que la resolución del DNS con LocalRoot, esa línea roja ya no se necesita porque el resolutor ya tiene toda esa información. No tiene que ir a preguntarle nada a la raíz. Sabe dónde está .COM, dónde está .ORG, dónde está .HORSES. Empieza después de eso.

Otra cosa que hace mi proyecto LocalRoot es que mantiene la caché del resolutor local actualizada y lo hace a través de notificaciones. Si se es esclavo de la raíz, se es esclavo de la infraestructura local solamente aquí. ¿Qué pasa? Cuando cambia la raíz, los servidores envían una notificación que dice: “Vengan a

buscar una copia nueva". Entonces los datos siempre están actualizados y no hay que preocuparse al respecto.

La pregunta es por qué la gente hace esto. Hay un par de respuestas. En el 7706 encontrarán más detalles de para qué sirve esto, en especial en lugares remotos donde hay mucho delay entre ustedes y los lugares remotos. Hay una pseudocaché de los datos de la raíz. Todo está en la caché. No es necesario contactar a la raíz ya. Se la saca de la ecuación. Se hacen lookups más rápidos de la primera vez que se busca un TLD así que la respuesta es milisegundos en la infraestructura local.

Otra cosa importante es que no solo los lookups son más rápidos sino que también se pueden buscar cosas que no existen. Si escribimos eBay y no le damos más información al navegador, la mayoría de los navegadores nos dicen: eBay esto, eBay aquello, eBay.com. Están buscando muchas cosas. La resolución negativa, el hecho de que .eBay no exista, bueno, la verdad es que no sé si existe, tarda llegar. Las respuestas negativas son más beneficiosas que la positiva porque las positivas están en la caché pero las negativas no. Al buscar al mes siguiente, no da la misma respuesta. Siempre tenemos una copia actualizada de la raíz.

Este es un proyecto en gran medida de investigación propia. Ustedes pueden hacer su propia investigación si quieren saber

cuánto hay cambios de la raíz o están desarrollando software. Es muy mecanismo en realidad para suscribirse a notificaciones del DNS en grupo.

Con respecto a la seguridad, lo mejor de DNSSEC y por eso estoy aquí hoy, es que como está firmado, ya no importa de dónde vienen los datos porque los datos DNSSEC, una vez firmados, están firmados por la IANA, yo se los puedo dar mal y ustedes pueden saber que yo se los di mal. Este concepto del LocalRoot es posible gracias al hecho de que los datos están firmados y todos podemos confiar.

Nosotros añadimos seguridad TSIG para que las notificaciones y las transferencias estén protegidas por TSIG. En este momento es obligatorio. Hay gente que dice que no se necesita TSIG. No voy a entrar en los detalles minuciosos de si es verdad o no esto pero puede ser que a futuro sea voluntario.

Ahora pasemos a hacer lo divertido de Adobe Connect, que es una demostración. Esta es la página principal. Lamentablemente, el tipo de letra es pequeño. En LocalRoot.isi.edu hay vínculos sobre el proyecto LocalRoot con mucha información. Si recién empiezan, hay distintos pasos para configurar el resolutor. Lo primero que tienen que hacer es registrarse con la dirección de correo y la contraseña, hacer procesamiento de captura si es necesario. Una vez logueados,

tienen que ir al proceso de registración con el código de registración y demás, y después hay algunas cosas que hacer en este sistema tan sencillo.

Lo primero es comenzar con los vínculos “Getting started”. Luego crear una clave para el TSIG. Les voy a mostrar cuáles son los pasos para configurar un resolutor después. Esta es la lista de claves TSIG. No hay nada en este momento que dice que todavía no se han generado claves y luego un botón para crear una nueva clave TSIG. Al hacerlo hay que llenar un formulario y ahí pueden poner lo que quieran, como nombre de la llave a nivel administración. En este caso, puedo poner mi divertida clave TSIG y cuando cliquean “Next” aparece la clave con el nombre del administración a la izquierda y aparece el algoritmo y el valor. No es necesario hacer nada con esto. Esto es todo automático. Después les voy a explicar la configuración. Es una lista de claves. No es necesario que copien el valor. Luego van a la lista de servidores, que son los resolutores. Tendría que cambiar esta palabra.

Son los resolutores recursivos donde vamos a desplegar la infraestructura del LocalRoot. Hay un botón para añadir un nuevo servidor y debajo hay solo tres campos que completar. El primero es el nombre administrativo del resolutor recursivo. Le pueden poner cualquier nombre. La mayoría le pone el hostname real y luego la dirección IP de donde se encuentra el

servidor. Está en versión v4. No sé si va a venir v6. Luego el TSIG que se va a usar. Como yo ya tengo una, me da esta pero si tienen múltiples claves, porque pueden poner la que corresponde, pueden tener granularidad regional. Luego cliquean en el botón “Create new server” y aparece la lista.

La letra es muy pequeña pero básicamente es lo mismo. Indica el nombre administrativo y la dirección, la clave TSIG y luego los tres estados Habilitado, que es la tilde, el botón Activo y Config. Enable significa que se puede activar y desactivar. Desactivar si uno no quiere más notificaciones.

El activo… Me he dado cuenta de que no quiero que la gente envíe notificaciones a todo el mundo, así que añadí una cierta protección. Para hacer una transferencia manual de tu dirección al servidor raíz antes de activarlo. Es para añadir seguridad. De hecho, hay un comando que pueden cortar y pegar del vínculo de “Getting started”.

Por último, el botón Config explica lo que hay que hacer. En este momento, la única config es para ISC bind. Espero que haya más en el futuro. No todos los resolutores recursivos soportan las transferencias XF unbound. Como es un resolutor recursivo específicamente, no puede implementarse. ISC Bind sí puede.

Después de que terminan esto, lo cortan, lo pegan y ya está. En la lista están todas las direcciones de donde pueden sacar

servidores raíz de backup. El primero es el B. Voy a ir añadiendo a medida que pase el tiempo más pero ustedes pueden sacar B, C, F, G y K y un par de sitios de ICANN también. Si alguno de estos quedara offline, aun así pueden estar operativos con los otros. Incluso si mi universidad decidiera descansar, relajarse, todavía tendría opciones. Los servidores están funcionando regularmente. Uno nunca se va a quedar sin operaciones.

Hablemos de los efectos ahora en el mundo real. Este soy yo desde mi casa. Yo tengo un resolutor recursivo en mi casa porque yo soy un geek, un fanático de la tecnología, y los picos son las queries por segundo. Fíjense que el pico llegó a 40-50. De repente, caen por completo. Eso pasó cuando activé los resolutores. Esos son los beeps desde mi casa y de repente hay muy pocos y eso es muy poquito. Después les voy a explicar por qué. La línea es plana porque ya no hablo con la raíz porque la raíz ya está localmente en mi casa. Después la apagué y la volví a encender. Hay muchas menos solicitudes a la red.

Lo importante, porque no es totalmente plano, hay algunos piquitos, es porque en la zona esclava cada tanto envía queries de registros DNS para verificar que sigue activo y que no está perdiendo notificaciones. Además, en mi casa está bypasseando el resolutor porque está midiendo la red. Hay un poquito más de tráfico en mi caso porque yo hago mediciones desde mi casa.

La siguiente diapositiva es la de las preguntas. Noté que hay un bug en la página, en el botón de login. Me parece que había un problema. No está bien. Lo tengo que arreglar. Me encantaría conocer qué opinan. Primero saber si les interesa, si lo usarían y lo probarían. Si ustedes hacen algún tipo de análisis, me gustaría saber cómo bajó el tráfico. Está este debate de que, como estamos bajando todos los datos de la raíz, aumentaría el tráfico y la velocidad porque no vamos a todos los TLD.

Si ustedes trabajan en proyectos de investigación, ya sea en datos o en notificación, me gustaría saber qué están haciendo y además saber qué otras funcionalidades les gustaría tener, qué otras características. En este momento lo acabo de terminar la semana pasada. O sea, todavía no hay botón para suprimir servidor pero va a venir. Dependerá de cuán popular es. Hay quienes lo consideran útil y lo quieren en su entorno local y otros no. ¿Alguna pregunta sobre LocalRoot?

CRISTIAN HESSELMAN: Soy Cristian. ¿Van a poder extender este concepto al nivel TLD?

WES HARDAKER: Lamentablemente no, porque no tengo conexiones con TLD. No sé si los TLD están dispuestos a hacerlo. Tendríamos que hablar con cada uno. La realidad es que hay muchos TLD. Estaría bien

llamarla no información propietaria sino información restringida. Sería interesante hablar con ellos. No sé si conviene tener todos internamente, porque sería demasiado ancho de banda.

ORADOR DESCONOCIDO: Están todos disponibles una vez al día.

WES HARDAKER: Hay un informe que contiene información de GitHub. Esa es una idea interesante. ¿Cuánta información podemos poner en la caché local? Es una buena idea.

ORADOR DESCONOCIDO: Tengo la impresión de que aunque la raíz cambia nominalmente una vez por día, las chances de problemas también son bajas.

WES HARDAKER: Sí, yo también pensaba que a futuro, para disminuir el ancho de banda, la realidad es que la raíz no cambia muy seguido. Se reasigna dos veces por día en general. Tres veces por día a veces pero es infrecuente. Yo opero la infraestructura de [ISI] para la raíz y sé que es infrecuente. Hay algunas firmas que cambian no obstante todo el tiempo. Lo que se haría es enviar una notificación al tercio del tiempo de expiración. También habrá

que hacer cierto bind, porque no se necesitan los datos tan seguidos. Tiene toda la razón. Ese es un proyecto posible de investigación para mí en el futuro. Si a alguien le interesa, bueno, mantengámonos en contacto.

RAED AL-FAYEZ: ¿Este concepto está aún en nivel de concepto? ¿Ya es una práctica? ¿Se puede poner en una red operativa? ¿Podría yo pedirle a mi ISP o a mi proveedor de telecomunicaciones que aplique este concepto? ¿Es seguro? ¿Es estable?

WES HARDAKER: Buena pregunta. Varias cosas. Este proyecto que yo creé, que permite recibir notificaciones y hacer sign up y config es muy nuevo. En la diapositiva dice alfa pero yo lo pasé a beta. Está en desarrollo. Habiendo dicho esto, de la manera en que desarrollé el config, permite que aun cuando el servicio falle aun así se van a recibir todos los datos de las raíces. El 7706, que es el concepto de hacer la caché de todos los datos al mismo tiempo, es una norma publicada y no es experimental. Creo que sí.

De todas formas, el config que les daré no se va a romper aun cuando yo me rompa. Yo podría decirle que desde ese punto de vista podría ponerlo en producción. Tengo que ver cuánto interesa y no tengo intención de desactivarlo. Cuánto desarrollo

haga dependerá de cuánto interés exista. Si le interesa, hágamelo saber y podemos intercambiar la idea por correspondencia. Mi dirección está en el sitio web al pie de la información. ¿Cuánta gente lo quiere activar? Levanten la mano.

ORADOR DESCONOCIDO: Yo tengo una pregunta. Con el tiempo hay más gente que hace esto, hay más recursores que hacen esto. ¿Qué significa en términos de infraestructura para la red?

WES HARDAKER: Se usará un poco menos. Una de las preguntas es cuál es la mejor manera de distribuir la información para la zona raíz. Esta es una de las opciones para que haya mejores maneras de utilizar estos queries especialmente. Se me puso en rojo el timer.

JACQUES LATOUR: A ver si hay alguna otra pregunta.

CRISTIAN HESSELMAN: Creo que si extendemos este concepto a nivel de TLD también se aumenta la resiliencia DDoS porque la información entra en las redes y puede ser DDoS pero también podemos trabajar en términos de resolución.

WES HARDAKER: El problema es que la información del TLD es más grande. La zona raíz es pequeña. No lo queremos hacer con .COM porque no vale la pena pero podría ser interesante para otros dominios que son más pequeños. Creo que es una buena idea. Agradezco esa opinión.

RUSS MUNDY: 7706 es informativa.

WES HARDAKER: Esa es una clasificación muy rara.

MOHAMMAD: Lo que veo en esa presentación es una transacción TSIG entre los servidores recursores y los de raíz. El administrador de la raíz debería configurar su servidor con una llave TSIG. ¿Esto es para todos los operadores?

WES HARDAKER: No. El TSIG es una llave compartida entre dos servidores de DNS o un cliente. Eso significa que es como tener una password compartida. Como cuando una persona tiene un password encriptado y la otra persona tiene que saber cómo desencriptarlo. Lo que hay que hacer es compartir la clave y no se trata de encriptar sino de proteger lo que no ha sido

modificado. La llave TSIG que se genera solo es buena entre mi servidor raíz local y el resolutor recursivo. No tiene nada que ver con la raíz. Yo recibo notificaciones de la raíz y en ese caso te las envío a ti. En este caso no hay que tratar con la zona raíz.

MOHAMMAD: El servidor es como un punto medio entre mi persona y el servidor raíz. Si el servidor raíz no funciona, ¿cómo llego a los otros?

WES HARDAKER: El servidor lo contacta una vez por hora para ver que no se haya quedado en el camino ningún dato. Si uno recibe una notificación, van a hacer un pedido en el SOA para que les dé una copia. Muchas gracias a todos.

JACQUES LATOUR: Tengo una observación. Estoy pensando. Si replicamos esto para el .CA donde podemos servir a una zona más grande, ¿con eso vamos a poder resolver el .CA? ¿Así podemos elegir a quién queremos? Esto quiere decir que potencialmente el requisito para una infraestructura [Anycast] tiene que ser supergrande y puedo tener una estructura suficientemente buena pero tenemos que ver cómo alinearla.

WES HARDAKER: ¿Cuántos registros hay en .CA?

JACQUES LATOUR: Dos millones.

WES HARDAKER: Con los códigos abiertos ahora lo podemos establecer pero te puedo dar la infraestructura si es necesario.

JACQUES LATOUR: Hay cosas que ver ahí. Gracias. El próximo orador es Vittorio Bertola, de Open-Xchange, que nos va a dar una presentación sobre DomainID utilizando DNSSEC para los sistemas de identidad digitales.

VITTORIO BERTOLA: Gracias. Este es un proyecto importante de Open-Xchange. Es una compañía que hace plataformas de webmail y aplicaciones de software como Power DNS. Tenemos el registro [.DE]. Uno de los efectos colaterales es que promocionamos el DNS y el DNSSEC y la idea es que podamos utilizar DNSSEC para las queries en este proyecto. Voy a ir bastante rápido porque esta es una parte general.

Todos ustedes saben que hay un problema en cómo las identidades son manejas en Internet. Tenemos demasiados nombres de usuario, claves, alguna gente usa gestores de password, otros usan distintos passwords debido a los distintos requisitos de passwords, no se pueden usar los mismos entonces también hay distintas demandas, etc. Todos están buscando una solución a esto y las soluciones son un sistema de sign-on único. Es decir, que uno tenga una única cuenta y se pueda loguear a cualquier cuenta.

Ya hay sistemas de sign-on globales regulares. El primer tipo de sistema es el que está en Europa. Tenemos un proyecto gestionado por el gobierno pero el problema es que son muy pesados y uno no quisiera dar el nombre verdadero y la dirección en este login. Entonces, a veces uno puede usar la idea oficial para la cuenta bancaria pero no para otros sitios. Lo que está despegando y que todo el mundo está empezando a usar hoy es esto. Los servicios de identidad global que nos permiten loguearnos con la cuenta de Google, de Facebook o de Twitter. Es muy útil. Todo el mundo lo está empezando a hacer. Nos parece que no es la forma en la que hay que hacerlo porque es propiedad de una sola empresa. La mayoría de las veces son empresas que monetizan esa identidad. Es decir, pueden llevarlas a otros sitios y no hay garantía de privacidad. Uno

tendría que tener la opción de poder usar más servicios. No solo esos dos o tres que aquí aparecen.

Lo que tenemos que hacer es crear un sistema de identidad pública. Por el momento tenemos lo que llamamos DomainID. Estamos buscando un nombre mejor. La idea es que tengamos un sistema de sign-on global que sea público, que tengamos un estándar que todo el mundo pueda implementar. Podemos tener millones de identidades diferentes y todas van a ser interoperables. Cualquier sitio web que acepte los login de este sistema puede usar y soportar cualquier identidad, cualquier proveedor e incluso se puede instalar el servidor.

En base a estándares públicos, queremos empoderar al usuario para que sea el usuario el que elija cuáles son los datos que quiere compartir con cada sitio web, que tenga distintas capas de control en las cuales el individuo las pueda compartir. Desde el punto de vista técnico, esto utiliza OpenID Connect, que es el protocolo que todo el mundo está usando. Estamos agregando varias cosas. Estamos construyendo a partir del DNS. El problema es que tiene que haber un proceso de descubrimiento. La idea es que podamos utilizar cualquier hosting o dirección de email como identificador para que se pueda poner el identificador en cualquier nombre de dominio. Luego se necesita un mecanismo para mapear la identidad hacia la entidad que la gestiona. La idea es que se va a utilizar un registro de DNS para

mapear la identidad del gestor. Lo que hacemos es que no solamente tenemos un proceso de descubrimiento sino que los propietarios de los sitios web pueden implementar un login y aceptar identidades de todos.

También ofrecemos portabilidad. La idea es que si uno no está contento con la empresa que está gestionando la identidad y uno no confía más en ellos puede mover el identificador a otro proveedor y luego continuar utilizándolo. Esto nos dará a los usuarios poder de negociación para que los proveedores de identidades no nos fuercen a utilizar la misma cuenta siempre. También tratamos de imitar la arquitectura del sistema de nombres de dominio en términos de la separación de roles, que no haya una sola empresa que sepa todo sobre nosotros sino que lo separemos en varias partes. Tenemos una autoridad de identidad que es el equivalente al registro de TLD y que es el que gestiona la autorización y autenticación. Es decir, que chequea cuáles son las credenciales que uno usa.

Luego tenemos un agente de identidad que es el equivalente al registrador, que es la parte que tiene la relación con el usuario. Es decir, como usuario, uno va a uno de estos agentes de identidad para contratar el servicio y se crea la autoridad de identidad. Uno puede dar o quitar el consentimiento en un mismo lugar, de manera que si uno cambia la dirección, no la tiene que cambiar 100 veces en distintos sitios web. También se

puede agregar más información sobre uno siempre que uno confíe en la única parte que conoce que es el agente. Se puede compartir a los distintos sitios web que están bajo el control.

Así funciona técnicamente. La idea es que uno usa cualquier alojamiento válido de DNS. Puede ser la misma computadora pero puede ser un servicio de streaming que uno no controla. El punto es que llegamos a este agente de identidad y para el servicio ellos posiblemente les den el nombre de dominio personal. Uno lo puede tener en la Telco, en el proveedor. Puede tener distintas empresas pero la idea es que uno tenga su propio nombre de dominio. Quizá con nombres de dominio, si no lo tienen, lo pueden comprar y empezar a gestionar registros de DNS. Utilizamos TXT record en d-mark style. Por el momento, esta es información muy básica, más allá de una versión de protocolo de identificadores decimos cuál es la autoridad de identidad y se puede hacer un query a partir del identificador. Los servidores tienen que ser contactados si uno quiere autenticar al usuario.

Esta es la parte de la creación. Por supuesto, se va a la autoridad. La autoridad verifica que esté configurado adecuadamente y al final el usuario va directamente a la autoridad de identidad. Debe conocer el pasaporte y también la clave. La clave tiene que estar asegurada. Uno puede utilizar incluso una password difícil porque es una especie de gestor de claves pero está online. El

agente y también el sitio web nunca pueden ver la clave. Por lo tanto, no puede robársela si uno no tiene intención de estar en otro lado o si tiene una password que esté craqueada.

Esto es lo que sucede cuando uno se tiene que loguear. Entra a un sitio web, pone su identificador y el sitio web solamente tiene que hacer una query de DNS para saber cuál es la autoridad y cuál es el agente. Esta es la parte que también está asegurada con DNSSEC y que ordena el uso de DNSSEC por política porque tiene que estar asegurada. Si no, puede ser atacado. El resto del proceso es estándar. Es el que ya implementamos. Tenemos implementaciones libres disponibles en los distintos servidores. No sé si ustedes aquí están familiarizados, quizá no con Adobe Connect pero hay un procedimiento donde el usuario se vincula con la autoridad y le pide al usuario la clave y lo tiene que hacer porque ya tiene una sesión abierta y en ese caso ya no hay que poner más la clave. La autoridad también puede implementar autenticación de dos factores. Eso está disponible para todo el mundo. Por lo tanto, es más fácil hacer que el login sea más seguro.

Después del login, el usuario va a dar su consentimiento para usar su información, especialmente si es la primera vez que se loguea. El sitio web va a tener un token de acceso para poder retirar ciertos datos. La idea es que la autoridad pueda utilizar todos los datos que el usuario está pidiendo y el usuario dice:

“Estoy compartiendo esto y no estoy compartiendo esto otro”. El usuario tiene el control total de la información que le da al sitio web.

Hay varias razones por las cuales creemos que esto es bueno para los usuarios. Primero, uno elige su identidad. Puede usar su nombre de dominio personal, puede elegir una empresa. Un no está obligado a ir al nombre de dominio de la empresa que está brindando el servicio. Uno puede ir a Facebook o a algún otro. También se puede elegir el proveedor y esto es muy importante porque es la manera de tener una relación incluso más segura entre los usuarios y los proveedores de Internet. Si se puede llevar o portar la identidad a otro proveedor, va a ser más fácil dar mejores servicios. Uno también puede elegir que los usuarios sean proveedores que no están monetizando los datos. En esta configuración inicial, en esta prueba de concepto, va a la autoridad, que no son compañías con fines de lucro. Por lo tanto, no tienen por qué vender tu información. Esto es un aumento en la confianza, incluso para los usuarios que no tienen tanta confianza en Internet.

Es más seguro también porque ahora hay un solo lugar que debe ser verificable porque allí es donde están todos los login pero no hay passwords. En todas partes hay que tener muchas passwords, escribirlas o ponerlas en un dispositivo o en algún lado. Incluso si el gestor es atacado o sufre un hackeo, lo puede

cambiar. Puede cambiar la autoridad de identidad y puede estar online de nuevo en cinco minutos. Esto tiene la intención de ser más privado. No hay ninguna razón por la cual no se deban tener múltiples identidades. La gente las usa para distintos servicios. Puede haber múltiples identidades gestionadas por distintos proveedores y ayudan también porque no hay una necesidad de registrar otros sitios web. Uno simplemente se loguea, la información ya está ahí y luego hay que comunicarla al sitio.

Se puede elegir qué información compartir. Es decir, se tiene el control de la información. Lo más importante es cuál es el valor estratégico para el trabajo y la industria de los nombres de dominio. La idea con esto es vender más nombres de dominio, que siempre es bueno, promoverlos pero también tiene la idea de promover el DNS y hacer que el DNS sea relevante porque esto es lo real para nosotros.

Sé que hay mucha gente en esta sala que está igual de asustada que yo por la dirección que está tomando el mundo en términos del trackeo, el rastreo de la presencia online y la privacidad. Desde un punto de vista, la capacidad de poder chequear la identidad de los usuarios es importante porque si tenemos una buena identificación en Internet, se puede atacar a distintos temas de seguridad, a distintos atacantes. Por otro lado, no tenemos que tener una Internet donde todo el mundo está tratando de jugar. Este tracking es la piedra fundamental de lo

que se está desarrollando ahora en Internet. Por eso nos parece que la capa de gestión tiene que volver a ser un estándar público. Tiene que ser interoperable por parte de distintos proveedores y usuarios, y no ser el campo de juego de algunas grandes compañías y proveedores.

La idea es que ahora el DNS es el directorio para alojar a los identificadores técnicos pero la información sobre las personas debe estar en el DNS. A nosotros nos parece que el DNS es excelente, la distribución del directorio. También es seguro al utilizar DNSSEC pero hay muchos de ellos que están comprando bases de datos, etc. Es decir, este es el momento de hacer lo que estamos imaginando. Ya vinimos trabajando en esto desde hace tiempo. Lo que queremos es tener un estándar público y abierto para que todos puedan dar y recibir identidades y loguearse con una sola identidad de todas partes y compartir los datos de un modo controlado y seguro.

Esto es lo que estamos generando. En este momento tenemos una prueba de concepto que está funcionando. Ya escribimos los primeros borradores y los hemos presentado hace un par de semanas. Ya están online y esperamos ver si hay interés y se puede estandarizar. Lo podríamos hacer. Quizá en parte esto debe estar dentro de la fundación de OpenID. Cumple con las normas de OpenID pero lo que más queremos es tener el feedback. Ahora estamos presentando el proyecto en distintos

lugares y queremos ver si la gente tiene una necesidad. Podemos participar y trabajar.

Tuvimos un buen feedback también de las Telco porque las Telco tienen un problema con el hecho de que ahora la gente se loguea con las identidades de Google y no con las suyas propias pero desde la comunidad de software hay mucha gente que está preocupada por lo que está sucediendo en términos de gestión de identidad. Aquí dejo para ver si hay preguntas. Pido disculpas por la velocidad. Si quieren les puedo explicar lo que deseen. Gracias.

ORADOR DESCONOCIDO: [inaudible], de [CZ.NIC]. Me gusta la idea. Quizá sepan que en [CZ.NIC] ya tenemos el proveedor para nuestros usuarios. Cualquiera que tenga un dominio puede tener una identidad en nuestro proveedor de conectividad abierta. Yo lo hice y funciona bien. Ya hemos hablado con Marcos de DNIC sobre esto. El diseño permitiría añadir fácilmente nuestro medio millón de usuarios de nombres de dominio y extender la base de datos.

VITTORIO BERTOLA: Eso sería fantástico. Estamos buscando los early adopters para promover la norma. Es necesario ponerlo desde una etapa inicial. Los proveedores son parte de la ecuación, la parte a

convencer pero si conseguimos una base de usuarios de los registros o de las telecomunicaciones, podríamos llegar a una masa crítica que invitaría a la gente a obtener más apoyo.

RUSS MUNDY: Gracias, Vittorio. Interesante el abordaje para aprovechar el DNSSEC. Mirando su presentación me vino a la mente que es claro que se requerirá cambiar los sitios. ¿Hay alguna idea en este momento? Pareciera que ustedes están sobre todo centrados en los sitios web. Las redes sociales y demás, ¿cuánto trabajo significaría para ellos participar en esta nueva ola de autenticación?

VITTORIO BERTOLA: Hay que saber cómo están implementadas las plataformas. Si usan OpenID no sería mucho esfuerzo. Es más una cuestión de saber si ellos quieren o no hacerlo porque estas compañías en general quieren conservar la identidad de sus usuarios. Estamos trabajando para que sea sencillo. Además, si el sitio está dispuesto a aceptar este nuevo sistema de identidad, nosotros brindaríamos apoyo. Hay que programar la query del DNS y eso no es tan difícil. Noto un interés en empujar esto hacia delante. Me parece que no sería un problema.

JACQUES LATOUR: ¿Alguna otra pregunta?

ORADOR DESCONOCIDO: [inaudible], del registrador alemán. Ayer se habló de tener un depósito de identidades y lo bueno es que el servidor lo permite hacer automáticamente. Cuando se hace login con Facebook como el primer paso es tan fácil y tan rápido, el dominio se registra en pocos segundos y luego se corren otras identidades. ¿Hay alguna idea de cómo hacer este primer intento de la manera más sencilla y conveniente para hacer funcionar el nombre? ¿Es sencillo?

JACQUES LATOUR: Yo ya añadí ese punto a mis especificaciones.

VITTORIO BERTOLA: Lo que se necesita es registrar el nombre de dominio. Luego está la cuestión de quién lo compra pero si está incluido en el servicio de router, ya viene incluido.

JACQUES LATOUR: ¿Quién hace la verificación de identidad real?

VITTORIO BERTOLA: ¿Usted se refiere a la indexización, a quién chequea si la identidad es real? Este es un protocolo de autenticación y la presunción es que todos los datos son autodeclarados. Yo digo: "Este es mi nombre", que es exactamente igual a cómo funciona ahora para la registración en línea. Podríamos tener algunos vínculos en el protocolo para verificar con terceros pero en la mayoría de los sitios creo que no es necesario probar que uno es uno. Para la mayoría de las cosas que uno hace en línea. En la mayoría de los casos, de hecho, uno quiere ser anónimo. Esto permite tal flexibilidad.

JACQUES LATOUR: Gracias. Buena presentación. El siguiente orador es Ondrej Filip, quien va a hablar de la administración automática del conjunto de datos.

ONDREJ FILIP: Buenas tardes. Soy Ondrej Filip. Soy de .CZ. Quiero mostrarles cómo creció en mi país. Tenemos más de la mitad de los dominios firmados en el registro pero la verdad es que son en su mayoría aquellos alojados en los mismos servidores del mismo registrador, que es básicamente una sola entidad. Consideramos que hay un 1% o 2% de otros dominios que están firmados y nunca publicaron sus registros DS, quizá por distintas razones. Quizá no puede presentar la clave. No sé. Las razones son

desconocidas pero hablamos con varios proveedores de DNS y ellos nos dijeron que no pueden presentarlos porque el titular del dominio no lo hace, no sabe hacerlo y son tantos registradores. Entonces, a veces hay apoyo de los registradores pero a veces los titulares de los nombres de dominio no entienden el DNSSEC. Es complicado. Los proveedores del DNS no tienen relación con el registro.

Otra motivación, que es la frase que puse, “Make DNS great again”. Hagamos nuevamente grande al DNS. Pido disculpas por usar esta frase del expresidente Ronald Reagan. Cuando se pone un dominio registrado, funciona para todo. No hay necesidad de tocarlo pero ahora con DNSSEC hay que refirmar las claves. Hay mucho trabajo que hacer y todo es muy complicado. Nosotros queríamos volver atrás y simplificar el DNS.

Por último, aunque no menos importante, estamos pensando en otros países que usan FRED y hacer open source. Instalar y desplegarlo en muchos otros países. Tenemos la responsabilidad de brindar ayuda a estos otros países. Lo queremos hacer lo antes posible. ¿Cómo hacerlo? Hay varias normas. Las principales son la RFC 7344, que introdujo los nuevos registros de DS y también la forma de trabajar con ellos. Recientemente la RFC 8078 que describe cómo hacer el bootstrapping del proceso y cómo remover los registros DS si uno no quiere eliminar el DNSSEC. Esto es muy importante.

También hay un borrador que creo que lo hizo… No sé. ¿Usted es uno de los autores? Muchas gracias por eso, que promueve el CDNS aquí en el registro. Quiero hablar de las dos caras del problema. Tenemos el registro y el software para DNS. El software de firma de DNSSEC. Estas son las listas de software de firma abierta, software abierto. El sistema del WHOIS de publicar la DNS key no está totalmente soportado en algunos de estos software. Creo que el plan de Open DNSSEC es tener a comienzos del año próximo. No sé si me equivoco.

PowerDNS y Bind tienen un sistema de publicación semianual. Hay que correr scripts de Chrome, no es automatizado pero casi. Knot DNS tiene soporte pleno desde la versión 2.5. Ahora estamos en la versión 2.6. Esta es la versión recomendada. Además, el software del registro, como decía, se llama FRED y también tiene soporte pleno.

Un poquito sobre Knot DNS. Uso traspaso de la KSK de firma doble. Se puede presentar opcionalmente la KSK a través de CDS y CDNSKEY y verificaciones periódicas de la existencia de registros DS a través de nameservers configurados. Pueden ser autoritativos o validadores. El servidor de nombres publica el CDNSKEY. Chequea que el registro DS está visible para el resolutor de validación y ahí hace el traspaso de la clave. Este es un ejemplo de configuración, como ustedes pueden ver. Se define la vida de la clave, quién comprueba la presentación del

registro CDNSKEY, del resolutor de validación y luego se configura la dirección del resolutor de validación y ese es el resto. Es automático el resto.

Otras funcionalidades que están en Knot DNS. Se puede hacer la firma de tipo único. También se puede tener clave compartida para varios dominios y no todos soportan el traspaso de algoritmos. Algo que quería mencionar especialmente, si se quieren suprimir registros DS, hay distintos tipos de CDS y CDNSKEY pero es algo que hay que hacer manualmente. Si se publican estas claves, esto significa que el registro DS se va a eliminar del registro.

Antes de empezar hablamos con los registradores, por supuesto, y les mostramos tres opciones. O bien no lo implementábamos, que siempre es una opción, no hacer nada, o los registradores lo iban a hacer ellos mismos, tomar los dominios y publicar sus registros, o el registro se iba a ocupar. No es de sorprender que a los registros no les interesó demasiado implementar algo nuevo y que dijeron: “Siga adelante usted. Ocúpese”. Ahora nosotros administramos los key sets, que es un cambio de concepto de cómo trabajan los registros pero parece estar funcionando bien. Esta es la arquitectura del registro. Nosotros tenemos algo que se llama CDNSKEY Scanner, que es un problema de C++, implementado en C++. Recibió la librería de [inaudible]. Muchas gracias. Es una lista de dominios. Lo que hace es chequear cómo

se distribuirán los queries, los distintos servidores de nombre, y luego intenta traer los nombres de servidores en su relación con la CDNSKEY.

Luego el software de administrador que se llama FRED AKDM, funciona en Chrome e invoca el CDNSKEY Scanner. Recopila los resultados y, si es necesario, hace algo en la capa correcta de FRED, que se llama FRED AKMD. Estas primeras dos partes no son específicas de registros. Se pueden usar en distintos registros. La última, FRED AKMD, es específica de un registro. Todo es open source y la buena noticia es que si alguien lo empieza a usar, es algo que ya está demostrado que puede ser utilizado universalmente. ¿Cómo funciona el escaneo? Escaneamos todos los dominios en la zone file para comprobar la existencia de registros CDNSKEY. Lleva unas tres horas. Mientras hace el escaneo, hay tres categorías de dominios. Aquellos que no tenían KeySet antes, sin registros DS en la zona antes. Aquellos que ya habían generado automáticamente algún key set, que ya estaban en el sistema y aquellos que tenían key set legados o definidos por los registradores.

Los pasos a seguir varían. Si no hay key sets anteriores, que es lo más complicado, porque pasamos de un entorno seguro a uno inseguro, escaneamos todos los servidores de nombres autoritativos. Utilizamos query de TCP y cuando se haya el CDNSKEY, le informamos al contacto técnico que la encontramos

y que creemos que es la señal para crear registro DS. Se sigue escaneando siete días más. Esto es algo que se describió en la RFC y nosotros pensamos que si alguien tiene control de la zona durante más de siete días utilizando TCP, es algo que puede estar fundamentalmente mal. Por eso entra en el proceso. Si el registro CDNSKEY es el mismo durante más de siete días, creamos registros DS, se registra en la base de datos y se informa nuevamente al titular del dominio por mail y también al registrador vía EPP. Ese es el primer caso.

El segundo caso es que se encuentra un dominio con un key set automático. Si se encuentra una nueva CDNSKEY que es una clave nueva que se actualiza, se implementa y nada más, es totalmente automatizado. No es necesario informar a nadie. Si el key set está vacío para la región, obviamente notificamos al titular del dominio y al registrador de que ha habido un cambio y el contacto técnico también es informado.

La última opción se llama el key set legado, el antiguo. Hay maneras seguras de ir al CDNSKEY, si es la clave regular creamos un key set nuevo automático y lo intercambiamos. Removemos el key set antiguo e informamos al contacto técnico por correo electrónico y al titular del dominio y al registrador por EPP, porque aquí hubo un cambio en el dominio. Antes era un key set estático y ahora está automatizado. Tenemos que informar que algo se cambió en la expectativa de que esté bien.

Algunas estadísticas. Comenzamos aproximadamente en junio. Desde entonces tenemos más de 600 dominios administrados así. Estamos recién empezando. Hay mucho más potencial. Hubo varios picos en el proceso cuando empezamos, cuando habilitamos el remplazo manual y pasamos al automatizado. Hubo varios picos. Hay una base de usuarios que está empezando. Va a crecer. Hay una diferencia entre los nuevos y los traspasados. El sistema encuentra cuál es cuál y provee el camino seguro hacia el registro. Es algo bastante sencillo y no hay más que hacer.

Estamos hablando en este momento con algunos de los registradores que lo podrían usar para sus propios dominios porque esto disminuiría las complejidades. Lo hicimos con dominios antiguos y no hubo problemas adicionales. Tenemos otras áreas de trabajo, otras discusiones. Yo estoy en contra pero hay quienes piensan que tiene que haber mecanismos para voluntariamente salir del sistema. Imagino que se va a seguir hablando porque si alguien publica un registro de DNSKEY, es una señal clara de que se quiere hacer DNSSEC pero se está debatiendo.

Algo más que probablemente vaya a incrementar la confianza en el proceso es tener más localizaciones de escaneo. Una única localización no alcanza. Planeamos extender a más sitios. Para mejorar la seguridad del proyecto, tenemos que mejorar la

notificación de los contactos, algo que ajustar, por supuesto. También queremos implementar el modelo push, que está en el borrador que redactó Jack. En este momento seguimos el modelo pull y queremos ir al modelo push en Knot DNS y en otras implementaciones. Si alguien lanza las claves, queremos hacer el push, enviarlo a los registros para que se genere automáticamente y que no sea que el sitio tenga que esperar días. Luego hacer algún tipo de marketing, hablar con los proveedores de DNS, que esta opción está disponible, explicarles que es la manera más sencilla de trabajar, que no va a complejizar la operación, etc. Esto es todo. Les agradezco. Quisiera saber si hay alguna pregunta.

JACQUES LATOUR: Gracias, Ondrej. Usted sabe que soy fan de todo esto. ¿Preguntas?

ORADOR DESCONOCIDO: Mi nombre es [inaudible]. Soy del registro .ID. Queremos ver implementaciones de FRED pero a veces no podemos encontrar una fuente alfa o beta para FRED. ¿Se puede usar un URL?

ONDREJ FILIP: Tengo buenas noticias. La principal arquitectura de FRED está aquí. Se llama FRED Knot. Ahí está todo lo que tiene que estar

disponible. Si no, simplemente traten de convencerlo para que eso ocurra. Esa debería ser la versión pero si falta algo, dígannos y vamos a tratar de mejorarlo.

JACQUES LATOUR: ¿Alguna otra pregunta? Yo sí tengo una pregunta. ¿Ustedes suponen que esa característica se va a habilitar por defecto?

ONDREJ FILIP: Está por defecto. Si usted registra un dominio en este momento y corre el KnotDNS con el sign-in, puede también correr DNSSEC.

JACQUES LATOUR: Si todos apoyasen esto, la adopción sería bastante rápida, ¿no?

ONDREJ FILIP: Sí. Si todos los servidores autoritativos lo permiten. Eso es lo que ayuda a la implementación porque, como dije, no aporta ningún beneficio operativo. Es para cualquier empresa que corra su propio DNS.

ORADOR DESCONOCIDO: Tengo un pequeño comentario. Usted dijo que hay unos 600 o 700 dominios. Quizá el 90% de esos dominios es de [Cloudflare] porque quienes apoyan este dominio gestionan el DNSSEC y en

el .CZ hay muchos más dominios pero hay mucha gente que todavía no hizo clic en el botón donde dice “Quiero DNSSEC”. Por eso estamos negociando con [Cloudflare] para ver cómo poner en el mercado esta característica para un cliente. Lo único que tienen que hacer es hacer clic en el botón. Lo segundo es si se van a poder pasar de opt-in a opt-out. Cualquier persona que se registre en [Cloudflare] va a poder tener DNSSEC disponible. Hay algunas cosas que son positivas, pero bueno, vamos a ir viendo.

JACQUES LATOUR: Muy bien. Gracias. Quizá este sea un tema para el próximo taller de DNSSEC. ¿Hay alguna otra pregunta? Muy bien. Gracias, Ondrej. Russ nos va a hablar sobre DNSSEC. ¿Cómo puedo ayudar?

RUSS MUNDY: Esta es nuestra sesión de cierre. Primero quiero agradecerle adicionalmente a todos nuestros presentadores de hoy y a todos aquellos que hicieron preguntas y que interactuaron. Esta es una de las razones por las cuales esta comunidad ha sido tan útil. Creo que también es una de las razones por las cuales DNSSEC ha tenido el éxito que ha tenido. Gracias a todos.

Si me pueden alcanzar el clicker, por favor. Esto probablemente no va a requerir todo el tiempo disponible pero de algún modo es un recorrido de las distintas cuestiones que todos en esta sala deberían identificar. Cada uno de ustedes tendría que encontrarse en alguna de estas diapositivas porque hay mucha cooperación en la comunidad. Tenemos un proyecto de investigación nuevo, que lo describió Wes, pero hay varios esfuerzos de investigación que son muy útiles. Ustedes van a ver estadísticas que aparecen varias veces. En este caso, para los operadores de TLD, sé que hay varios operadores de TLD en las reuniones de ICANN, nosotros empezamos la sesión hoy diciendo que el 90% de los TLD están firmados pero todavía hay más por hacer.

Es decir, cualquier operador de TLD que no firmó su zona, trate de hacerlo. Si necesitan ayuda o aporte de alguna otra persona, este es un buen lugar para recibirla porque hay muchas personas que van a estar contentos de compartir lo que aprendieron. Por supuesto, también tienen que estar listos para aceptar los registros de DNS y las claves de DNS porque van a ir moviendo el DNSSEC por la jerarquía. Hay algunas áreas en las que los registradores han hecho un excelente trabajo pero en muchos TLD todavía hay un desafío y es que el registrador no está preparado simplemente por varias razones, para hacer cosas con DNSSEC. Esta también es una de las razones por las cuales

esta iniciativa es tan diferente. Las iniciativas de Ondrej y otros son muy útiles pero hay muchos lugares donde lograr que los registradores participen. Haría una gran diferencia.

Estadísticas, estadísticas, estadísticas. Hay muchas personas que necesitan y quieren contar e identificar qué es lo que sucede para que podamos ver cuánto avance se ha logrado. También una muy buena ayuda en términos de la implementación de la llave. Para los operadores de zona, pueden operar en cualquier zona que está en la casa. Yo diría que esta sala puede contener un porcentaje más alto de personas que están operando resolutores recursivos que otras casas en cualquier otra sala en el mundo, pero hay otros lugares. Los podemos mirar profesionalmente, lo que ustedes están haciendo con su trabajo o si ustedes conocen a otra gente que opere en zonas, hagan la verificación de DNSSEC con ellos. Díganle al registrador que ustedes quieren apoyo porque muchos todavía no lo quieren. De nuevo, estas son las estadísticas.

Empresas. ¿Qué pueden hacer las empresas de Internet para lograr que el DNSSEC se expanda y se extienda un poco más? A nivel de empresa, no tenemos nada útil para medir qué es lo que sucede pero todavía hay una cantidad muy pequeña de usuarios de DNS a nivel de empresa. Fíjense cómo esto se puede usar en sus lugares de trabajo. Hablen con su gente en el área de

seguridad, en las áreas que están preocupadas por el riesgo, la evaluación de riesgo. DNSSEC puede ayudar en ese sentido.

Cuando ustedes están hablando con los ISP, ahí es donde esos ISP y la validación se convierte en algo muy, muy importante. La mayoría de la gente no tiene resolutores en su casa. Ellos confían en sus ISP y, si no están usando alguno de los validadores de ISP, como los que mencionó Google, Verisign tiene algunos y hay resolutores de validación que la gente puede usar pero es incluso mejor si uno puede lograr que el ISP local lo haga. Cada ISP tiene zonas en sí y ellos tienen que firmar su propia zona y que participen completamente.

Cada uno de nosotros aquí puede hacer algo más para sí mismo. Hay una gran parte de la gente que viene a nuestros talleres. Les gusta meter los dedos si no en el código, al menos en la operación o en configurar sus propias máquinas o construir su propio entorno local, experimentar. Yo creo que muchas veces las lecciones que terminan siendo utilizadas e incorporadas a nivel global terminan en el IETF pero empiezan con ideas que vienen de conjuntos individuales. A veces algunos simplemente hacen experimentos con sus propias redes en casa.

Quisiéramos tener más lecciones aprendidas. Ya llevamos más de 10 años haciendo nuestros talleres de DNSSEC y sigue habiendo interés de mucha gente. Lo que queremos es ver que

esto continúe o planear hacer algún otro taller en la próxima sesión de la ICANN. Vamos a anunciar el llamado a la participación posiblemente en diciembre o a principios del año que viene. Queremos escuchar lo que tienen para decir todos y ver cuánta ayuda se le puede brindar a más gente.

Talleres, entonces. Otras reuniones. RIPE está haciendo mucho en su espacio. Sé también que en Japón y JPRS están haciendo mucho. Por eso en sus áreas locales traten de organizar cosas. Rick Lamb ha estado en esta área dando cursos. Esta es una muy buena manera de aprender y de participar. De nuevo, gracias a todos los que estuvieron aquí y que participaron. Un agradecimiento más a nuestro sponsor del almuerzo, Afilias, CIRA y SIDN.

Tuvimos un buen apoyo. Como dije, hace más de 10 años que estamos haciendo los talleres. Eso no sería posible sin el apoyo del SSAC, que es uno de los comités asesores de ICANN. También del programa 360 de la Sociedad de Internet. Tenemos algunos pointers y URL para que ustedes puedan llevarse más información. Quisiera dar un agradecimiento especial a [Julie] y a Cathy, que hacen que todo esto sea posible para nosotros. Muchas gracias. Una oportunidad más. Está la abierta la sesión de preguntas y respuestas, si quieren hacer un comentario o decir algo que estaban pensando.

WES HARDAKER: El botón de log-in que no funcionaba, ahora sí funciona.

RUSS MUNDY: Muy bien. Ahora contamos con la máquina de Wes.

ORADOR DESCONOCIDO: Wes, usted dijo que informativo era un estatus raro para el 7706. ¿Cuál cree que debería ser?

WES HARDAKER: Es una muy buena pregunta. La realidad es que cuando yo dejé de pensarlo, dije: "Quizá sea verdad". Podría ser experimental. Eso sería razonable pero no es un cambio de protocolo sino que tiene que ver con cómo uno implementar algo. Lo podría haber hecho antes pero es simplemente documentar el hecho que es una solución disponible especialmente en los entornos bajo ancho de banda.

RUSS MUNDY: Muy bien. ¿Hay alguien más que tenga un pensamiento final? De nuevo entonces, gracias a todos. Se lo agradecemos mucho. Esperamos ver a muchos a ustedes la próxima vez.

[FIN DE LA TRANSCRIPCIÓN]