ABU DABI – Reunión conjunta de la Junta Directiva de la ICANN y el Grupo de Expertos Técnicos (TEG)
Miércoles, 1 de noviembre de 2017 – 17:00 a 18:30 GST
ICANN60 | Abu Dabi, Emiratos Árabes Unidos

DAVID CONRAD: Quisiera invitar a los demás miembros de la junta que están aquí a que por favor vengan a la mesa. Tenemos algunos asientos libres. Hay otros miembros de la junta que están allí y aquí hay lugar en la mesa. Gracias, Markus y Becky.

Bueno, supongo que podemos comenzar. Bienvenidos a esta reunión del grupo de expertos técnicos. Una serie de expertos técnicos que se reúnen con la junta directiva de la ICANN. Especialmente este año tenemos algo un poco nuevo con la Creación del Comité Técnico de la junta directiva. Este comité creo que debe asistir a esta reunión. Es una reunión obligatoria. No podrían dejar de asistir aun si quisieran no estar aquí. Por una cuestión de tiempo, mis comentarios van a ser breves aunque quisiera señalar especialmente el hecho de que la razón por la cual uso corbata hoy no es porque vaya a hacer una entrevista sino en honor a la última reunión de Steve en el Grupo de Expertos Técnicos. Por supuesto, podrá seguir participando en el Grupo de Expertos Técnicos en el futuro, si así lo desea.

Personalmente, quería decir que valoro muchísimo todo el trabajo que hizo Steve. De hecho, la creación de este grupo

estuvo impulsada por él. Mágicamente yo terminé a cargo. Quiero agradecer a Steve por todos sus esfuerzos y por haber mejorado el nivel técnico de la organización y por ayudarme a mí, un simple director de tecnología, a mejorar la tecnología en la ICANN. También quiero agradecerle por muchas otras cosas que hizo. Habiendo dicho esto, a menos que quiera decir algo…

STEVE CROCKER: Gracias por sus amables palabras. Usted ha trabajado muchísimo. Creo que marcó una gran diferencia. La buena noticia es que usted sigue estando aquí. Este grupo, el Grupo de Expertos Técnicos, es un grupo con el que estoy muy satisfecho. Surgió de una manera inesperada pero creo que agregó experiencia y conocimientos además de creatividad y un lugar para determinados debates que, de lo contrario, no tendrían lugar en ningún otro lugar. Por lo tanto, me alegra mucho que se haya creado este grupo y que tenga una cierta vitalidad.

Espero poder compartir esto con la gente que está aquí. Yo lo compartí con todos ustedes. Este es el mensaje. Continúen con esto. Esto es muy bueno. David, realmente encargó los aspectos administrativos y también la parte de la agenda creativa importante. Se ocupó de reunir a las personas, etc. Es muy bueno.

DAVID CONRAD: Muy bien. Habiendo dicho esto, creo que podemos empezar ahora con el contenido de la reunión. La primera presentación estará a cargo de Fernando López, quien va a hablar acerca de los identificadores persistentes del estilo DOA. Será una demo. Es una prueba de concepto que utiliza identificadores persistentes similares a lo que se describe en algo que se llama DOA o Arquitectura de Objetos Digitales que se implementaron como una aplicación sobre el DNS. Creo que esta presentación será en español. Las intérpretes harán la traducción al inglés. Parece que Alain quiere decir algo.

ALAIN DURAND: Gracias, David. Voy a presentar las primeras diapositivas que nos llevarán a la demo. Voy a hablar en inglés.

DAVID CONRAD: O su versión del inglés.

ALAIN DURAND: Puedo hablar en francés también. No sé si me entenderé a mí mismo. ¿Tenemos las diapositivas?

DAVID CONRAD: ¿Podemos pasar a las diapositivas y sacar la hoja con el resumen?

ALAIN DURAND: Voy a comenzar con algunas aclaraciones. Eso es un trabajo que inició la oficina del director de tecnología de la ICANN. El objetivo es demostrar si los identificadores persistentes del tipo DOA podrían utilizarse sobre el DNS. Esta presentación entonces va a referirse al estado del prototipo que hicimos en colaboración con la Universidad de la Plata y Fernando va a hablar sobre este tema más adelante. Esto no es un apoyo a las tecnologías de la DOA por parte de la organización de la ICANN. Quiero aclarar esto.

El contexto de persistencia es el siguiente. Se ha sostenido que los URL pueden quebrarse o caerse por diferentes razones: cambios en las organizaciones, cambios de nombres de empresa, fusiones y adquisiciones. Después de 12, 18, 24 meses, hay una serie de URL que terminan fallando. Hubo una serie de soluciones en la industria para este problema, como redireccionamiento de URL.

La solución de DOA consiste en considerar a los identificadores persistentes. La idea es tener prefijos que son números. Al no usar nombres, al no usar algo que tiene algo semántico o mnemónico, lo que se sostiene es que si cambio la organización, el número sigue siendo el mismo. Si tenemos un nombre, uno puede querer transmitirlo o no a la nueva organización. Si es un

nombre, ya no importa tanto. Del lado de los sufijos, en lugar de tener esta estructura profunda que refleje en cierta forma la estructura interna de una empresa, recomendamos utilizar el espacio plano, sin jerarquía.

El sistema Handle utiliza protocolos específicos que no están estandarizados en organismos de estándares abiertos como el IETF. Si uno los mira, no parece que estos protocolos pudieran agregar nada a la historia de persistencia. La persistencia en realidad es el resultado de una convención de nombres. ¿Podemos hacer esto con el DNS? Nuestra respuesta breve después de ver esto durante unos meses es sí. Necesitamos tres cosas. Un lugar en DNS para anclar todo esto. Lo vamos a llamar Persistency Anchor o PANCHOR. No necesita ser uno solo. Pueden ser varios para permitir la competencia. Necesitamos una convención de nombres que sea similar a la descrita anteriormente en las etiquetas de DNS no utilizamos mnemónica. No utilizamos nada que tenga una semántica. Podemos utilizar un número, un hash, pero nada que sea mnemónico. Tampoco hay que mapear la estructura de organización. Se utiliza en este sentido una estructura lo más plana posible.

En tercer lugar, utilizamos un nuevo tipo de RR. Tenemos que incluir un nuevo tipo de registro. Lo llamamos DOARR pero este fue el primer intento. Seguramente le vamos a cambiar el

nombre. Estamos pensando en llamarlo DT, por datos. En este tipo de registro vamos a poner un objeto de una estructura que es algo que contiene cierta información que no necesariamente tiene que ser un mapeo. Puede ser toda clase de información.

Este es el tipo de registro. Contiene datos de la empresa, tipos de datos. Este es el número que la IANA les asigna a las empresas. Si uno quiere tener su propio tipo de datos privado, lo puede poner ahí. El segundo campo es el tipo de datos. Pueden ser valores predefinidos o definidos por el usuario. ¿Hay una localización? Los datos van a estar dentro de registro o habrá un puntero que nos llevará a los datos. Un tipo de medio puede ser por ejemplo texto codificado con determinados conjuntos de características o puede ser binario, lo que ustedes quieran. Si hay datos, entonces podemos incluir los datos ahí, sabiendo que no puede ser demasiado grande para que entre dentro del registro del DNS. Vamos a la próxima, que es la más importante.

Nosotros pensamos en un prototipo y cuál es el uso de este prototipo. Pensamos en el dominio de Internet de las cosas. Escuchamos hablar mucho acerca de Internet de las cosas e identificar el sistema en función del tipo de dispositivo. Pensamos en una empresa que se llama BigCo. BigCo está creando dispositivos para Internet de las cosas. Tenemos este Persistency Anchor. Le damos una etiqueta a esta empresa que es la etiqueta 12. La empresa produce dispositivos y para esta

clase de dispositivo en particular le asignamos un nombre. 78902. Son números inventados para que tengan un ejemplo de lo que podemos poner en esos registros. Para describir una empresa, podemos tener una página web que apunta a cierta información sobre la empresa, contacto, dirección de email, la clave pública asociada a una empresa que describe el objetivo, el modelo de dispositivo de hecho. Podemos hacer lo mismo pero también tenemos cosas más interesantes. Por ejemplo, el firmware o la firma del firmware o la versión del firmware para que el dispositivo que busque esto se dé cuenta de si estoy usando la versión correcta del software. De lo contrario, habrá un puntero que me llevará para descargarlo. Vamos a hacer una demo ahora. Le voy a dar la palabra a Fernando.

FERNANDO LÓPEZ: Voy a hablar en español. Soy Fernando. Soy de la Universidad Nacional de La Plata. Soy docente e investigador allí. Siguiente diapositiva. Un equipo en la universidad por intermedio de Cabase se puso a trabajar en crear una demo, una aplicación para registros DOA. Siguiente. Siguiente.

En principio, Cabase registró el dominio persistent.lat. El CESPI, que es una entidad de la Universidad de La Plata, configuró un conjunto de servidores para servir nombres dentro de ese dominio. Los servidores que estamos usando, que proveen

registros DOA, son una versión beta de BIND pero no tienen ninguna modificación especial. Solamente es una versión beta. Ahí implementan DNSSEC. Siguiente.

Para la parte de dispositivos, que es la parte donde desarrollamos la demo, trabajamos con unos dispositivos que se llaman NodeMCU. Utilizan un microcontrolador de bajo costo que integra wifi, que se llama ESP8266. El costo de estos dispositivos, incluyendo una antena y una memoria flash ronda el $1.50 en volumen. Son programados normalmente en C++ o distintos lenguajes.

Para implementar la demo, lo que tuvimos que hacer es modificar la librería LWIP, que es la librería que le da soporte de red a estos dispositivos. Dentro de esa librería modificamos la parte de DNS para que pueda enviar peticiones DOA con el tipo de registro 259 y recibir y procesar las respuestas. Siguiente.

La demo, la vamos a cortar un poco, originalmente consistía primero en configurar el registro. Ahora vamos a tomar el registro ya configurado como está en el paso uno. Vamos a saltar al paso tres en el cual el dispositivo va a arrancar y al arrancar va a hacer una petición por un registro DOA. Va a recibir desde el servidor la respuesta y dentro de la respuesta va a recibir cuál es la versión más nueva de firmware disponible, un link a esa versión de firmware y una firma del firmware. Luego, si el

firmware disponible es más nuevo que el presente, va a proceder a actualizarse automáticamente. ¿Podemos ir a la pantalla compartida?

Esta es la foto del dispositivo que les voy a mostrar y la interfaz de configuración. Esta parte la vamos a saltear. ¿Podemos ir a la pantalla compartida? Por favor, esperen un segundo. Bueno, del lado izquierdo de la pantalla vamos a ver el proceso de arranque del dispositivo. Yo lo tengo conectado por USB a mi máquina para poder ver los pasos del arranque y poder detenerlo en cualquier paso. Del lado derecho vamos a ver una captura de tráfico de las consultas DNS y las respuestas. En rojo van a aparecer las peticiones de DNS y en azul las peticiones DOA, las respuestas con registros DOA decodificados.

Ahí está el primer paso. Hace la consulta. Dentro de las respuestas tenemos el campo de descripción, que lo vamos a ignorar para este caso. Campo de firmware con la URL de dónde descargar el firmware más nuevo. El campo de versión. Un email de contacto y el campo de la firma. La parte de la captura está ralentizada. Está más lento de lo normal para que podamos ver los campos pero aquí se puede ver que el firmware ya recibió toda esa información. Si paso al paso siguiente, va a empezar a descargar el firmware para actualizarse. Esto toma unos segundos. Después se reinicia y ya arranca con el firmware nuevo.

Dependiendo de la conexión, puede tardar algunos segundos más. Está cargando la actualización. Mientras les puedo contar que la modificación realizada es relativamente pequeña. Para hacer una implementación en C son 300 líneas modificadas. Fue una semana de investigación para entender primero DOA y para entender la librería LWIP y luego solamente tres días de implementación. Del lado izquierdo pueden ver cómo el dispositivo ya se actualizó, se reinició y está anunciando que tiene la versión nueva, la versión 1.0.

ALAIN DURAND: Muchas gracias, Fernando. Quisiera agregar algo. Cuando tratamos de hacer estas demos en vivo, tuvimos algunos problemas en la red y cuando pasamos a IPv6 para hacer esta red, funcionó bien. Quiero agradecerle mucho a la gente de la Universidad de La Plata y a la gente de Cabase que nos ayudaron a preparar esta demo en solo tres semanas. Este es el dispositivo del que estamos hablando. Cuesta $1.50, dependiendo de cuántos compremos.

DAVID CONRAD: ¿Hay alguna pregunta? Sí, tenemos cinco minutos para preguntas. De hecho, Steve tiene una pregunta para comenzar.

STEVE CROCKER: La actualización automática me llama la atención. Obviamente es algo muy bueno a menos que la actualización ocasione algunos problemas y uno pierda control del dispositivo. ¿Cómo describen las propiedades de seguridad para que las actualizaciones no nos dejen en una situación peor de la que estábamos?

FERNANDO LÓPEZ: Este dispositivo especial puede actualizarse y solo toma la actualización si el firmware es válido.

STEVE CROCKER: De esta forma se cubrirían los errores en la red. ¿Qué ocurre si la actualización propiamente dicha tiene un bug?

FERNANDO LÓPEZ: En ese caso es necesario implementar otra solución como un reset físico o algo así.

ALAIN DURAND: Quiero señalar que este no es un producto. Es una prueba de concepto. Hay diferentes cuestiones que habría que resolver en caso de que fuera un producto.

STEVE CROCKER: Me gustan las pruebas de concepto.

DAVID CONRAD: Dave, Jonne y Rick.

DAVE PISCITELLO: En primer lugar, esto es fantástico. Gracias por implementarlo. Me encanta el hecho de que haya logrado explicar algo que es muy difícil de explicar y que lo haya podido implementar en muy poco tiempo con una gran claridad. ¿Pensaron ustedes que en lugar de centrarse en el nivel de los datos traten de trabajar en el nivel de objetos para tener una registración dinámica del dispositivo como parte de la interacción? Si hacemos esto, básicamente estamos capturando los botnets. Si sabe lo que es un dropper file en una infección con malware, podríamos tener el equivalente de un dropper firmware en cualquier cosa que pongamos en una red de Internet de las cosas. Lo único que podría hacer el dispositivo sería usar el DNS para ir, enrolarse y luego recibir instrucciones. Lo mismo que si viniera de un command y un control. Veo una enorme oportunidad para tomar el DOA y llevarlo en esa dirección. Quisiera sugerir que en lugar de que lo llamen DOA o DTA, lo llamen OBJ, objeto.

ALAIN DURAND: Gracias. Es impresionante. Sí, puedo responder rápidamente. Hemos estado pensando exactamente en lo que usted sugiere porque cuando mostramos la delegación a la empresa y la empresa al modelo de objetos, tenemos una capa más de delegación hacia el número de serie. Podemos delegar esto para que sea administrado hacia el objeto y utilizar DNSSEC para validar. Quiero recordarles que en esta demo todas las zonas han sido firmadas con DNSSEC.

ORADOR DESCONOCIDO: Lo que usted está describiendo en una modificación del sistema de DNS para que se pueda trabajar con DOA pero en este momento el sistema de DOA está utilizando DNS. Estamos hablando de doa.org/ flat space (espacio plano). El tema de la persistencia no es un problema para el DNS. Es un tema de política dentro de la organización pero el URL sigue funcionando y doa.org es tan estable como cualquier otro registro que produzca el sistema DOA. Me pregunto por qué eligieron modificar el sistema de DNS dado que están utilizando las raíces de DNS. Es decir, la implementación del DNS de la ICANN.

ALAIN DURAND: Gracias por la pregunta. No estamos modificando el sistema de DNS. Lo que hemos hecho es crear un nuevo tipo de RR. No cambiamos los servidores ni los resolutores ni ninguno de los

miles de elementos de DNS que existen. Solo creamos un nuevo tipo de RR. Para describirlo, le pedimos al equipo de implementación que lo hiciera y en una semana ya teníamos cuatro implementaciones.

En cuanto al segundo comentario, con respecto a que el DOA utiliza el DNS, lo que hace es utilizar un proxy. Envían todos los datos a través de [ICTP] pero después lo transfieren al sistema Handle. Estamos pensando si podemos evitar esto, evitar los proxy y los temas de privacidad relacionados con los proxy y con tecnología. Decidimos hacer algo con la tecnología de DNS simple que hemos utilizado durante 40 años.

DAVID CONRAD: No sé si hay otra pregunta. Cerramos la lista de personas que pidieron la palabra porque tenemos poco tiempo. Jonne.

JONNE SOININEN: Quiero subrayar lo que dijo Alain. La demo no tiene que ver con actualizar los dispositivos. La demo tiene que ver con utilizar el DNS como función al DOA, sin modificar nada a nivel de la implementación. Además de esto, obtenemos todas las ventajas, incluso un pequeño dispositivo que tiene DNS. Esto no causa un problema a la capacidad de estos dispositivos sino que se

pueden correr los protocolos tradicionales en un paquete muy pequeño y con muy poca implementación.

De hecho, no es una gran sorpresa de alguna manera porque DNS y todo lo que se hizo por los protocolos de IP fueron desarrollados en una época en que probablemente lo que tenemos en la mano hubiera necesitado mucho más espacio y se hubiera llamado computadora de escritorio. Este es un excelente ejemplo de que realmente deberíamos considerar lo que ya tenemos hoy y pensar en las nuevas formas en que se puede utilizar.

ALAIN DURAND: Muchas gracias.

DAVID CONRAD: Rick.

RICK LAMB: Maravilloso. Realmente me gusta mucho ver esto. Yo también soy un usuario de ESP826. Los mismos chips. Tengo una pregunta. ¿Ustedes modificaron la pila de LWIP para que soporte DNSSEC? Estas búsquedas, ¿están validadas?

FERNANDO LÓPEZ: En este momento no verifica nada con DNSSEC.

RICK LAMB: Eso sería interesante. Eso se utiliza en todos los dispositivos de IoT que existen en el mercado.

FERNANDO LÓPEZ: Eso sería interesante para esta solución pero todavía tenemos que hacerlo.

ALAIN DURAND: Todo esto empezó inmediatamente después de la reunión de LACNIC hace tres semanas. Yo estuve hablando con mi amigo de Cabase y dijimos: "Intentemos hacerlo". En lugar de volvernos a casa después de la reunión de Montevideo, me tomé el barco y fue a Buenos Aires. Al día siguiente me dijeron que fuera a la Universidad de La Plata para ver si podíamos hacer esto. Teníamos tres semanas. Tuvimos que hacer el mínimo posible para que funcionara. Etapa dos, queremos hacer lo que usted dijo. Queremos hacer lo que está diciendo David. No hay nada que nos impida hacerlo porque es bastante simple.

DAVID CONRAD: Asha.

ASHA HEMRAJANI: Gracias. Impresionante. Considerando lo que acaban de decir. Además de actualizar dispositivos, otro desafío con los dispositivos de Internet de las Cosas es la autenticación a fin de que se verifiquen correctamente las credenciales. ¿En qué medida sería simple incluir esto o incluir la autenticación del dispositivo?

ALAIN DURAND: Creo que se puede aplicar a muchas cosas. Podemos hacer autenticación del dispositivo pero podemos pensar en otros tipos de aplicaciones que necesitan un identificador persistente. Me han estado hablando de historias clínicas, por ejemplo. Podemos hacerlo. Esto es algo que utiliza la tecnología de DNS no para mapear nombres, conexiones de IP, que es lo que normalmente se piensa, sino como una forma de trabajar. Tenemos un identificador que puede ser todo lo persistente que quieran y es un buen punto para que este objetivo llegue a donde quiere. Ustedes deciden a qué quieren que apunte. Se puede utilizar en muchos, muchos campos diferentes.

JAY DALEY: Estoy tan confundido como horrorizado por esto. Yo creo que la DOA, la Digital Object Arquitecture es una tecnología con un modelo de gobernanza muy pensado y un modelo de propiedad intelectual muy bien pensado y analizado. Además, tiene

muchos problemas. Yo creo que habría que ver qué pasa con la gobernanza porque hay otros elementos que no van a verificarse y corregirse tan fácilmente. ¿Qué va a hacer la ICANN al respecto con todos estos problemas que tenemos?

DAVID CONRAD: Una de las actividades que está desarrollando la oficina del director de informática es analizar la tecnología de nuevos identificadores. La DOA es una tecnología que ha generado cierto interés en diferentes foros. Parte del proyecto tiene que ver con entender qué es la DOA y cómo funciona y su modelo de gobernanza. Una de las cosas que identificó Alain al hacer sus investigaciones sobre DOA era que aparentemente no cambiaba mucho. La tecnología en sí misma es una tecnología de asignación de nombres pero está incorporada en un modelo de gobernanza diferente que desde nuestro punto de vista no es necesario. Parte de este trabajo tiene por objeto demostrar que en la actualidad esto no es necesario. El modelo de gobernanza está actualmente separado de la tecnología. Por supuesto, la tecnología se puede implementar sobre el DNS. No hace falta el modelo de gobernanza. Eso es parte de la demostración de esta tecnología y el punto que estamos tratando de entender. Es decir, qué hacía la tecnología y cómo lo hacía para asegurarnos de que realmente podíamos comunicar esta información a la comunidad.

DAVID CONRAD: Creo que ahora es el momento de pasar a la próxima presentación.

LEONARD TAN: Yo soy Leonard Tan. Hoy voy a hablar sobre el servicio de nombres Ethereum. Para aquellos que no conocen lo que son las cadenas de bloques, les voy a dar una descripción. Las cadenas de bloques son mayores distribuidos y como todos los libros mayores, tienen números positivos y negativos. Esto se ha implementado en el pasado a través de otros modelos. Las cadenas de bloques tienen mejores resultados. Se utilizan en todo el mundo. Los bitcoins por ejemplo y compensan los costos de verificar. También esto desincentiva los ataques.

Ya sabemos cómo funcionan las transacciones. Todas las transacciones tienen una entrada y una salida. A fin de que una transacción sea válida, se debe hacer una referencia a una salida anterior. ¿Cómo son las transacciones? Como esto. Las transacciones se refieren siempre a una transacción anterior hasta un bloque de mina donde se crea el primer bitcoin. La segunda transacción se refiere a la anterior. Cada transacción tiene una producción, una salida que utiliza una clave pública. Está bloqueada con una clave pública. En este sistema no sabemos si los usuarios gastan dos veces su dinero, si la

transacción está correctamente formateada. Solo tenemos una serie de transacciones, 2.000 por bitcoin, por ejemplo. Se verifican todas siguiendo estas reglas. Después se trata de poner una hash en este bloque en un umbral y cuando se llega allí, se recompensa a los participantes con un bitcoin.

Ethereum es como los bitcoins, una cadena de bloques. En lugar de almacenar datos y monedas, también podemos hacer computaciones en cadenas de bloques Ethereum. ENS es un sistema relacionado con Ethereum. Primero voy a hablar de por qué tuvimos que crear ENS y después cómo funciona y después le voy a decir cuál es la situación actual. ¿Qué es ENS? Básicamente es una forma de mapear nombres legibles por los seres humanos con los recursos. El problema aquí es que esto está expuesto a ataques de phishing. En ENS podemos referirnos a registros y direcciones y contratos utilizando nombres. Además, también podemos utilizar ENS para referirnos a otro tipo de registros como registros de IPFS y Swarm. Incluso claves públicas para verificación de identidad. A nivel más alto, podemos pensar en ENS como un servicio de búsqueda distribuido. Resiste a los ataques DDoS y como las transacciones se hacen en cadenas de bloques, son transparentes. Además el sistema también se puede actualizar.

La arquitectura interna de ENS está dividida en dos componentes. El registro ENS y los resolutores. El objetivo

principal de registro ENS es mantener un mapeo entre nombres y propietarios y resolutores. Si ustedes son los propietarios de un nombre, pueden hacer tres cosas. Número uno, pueden cambiar al propietario, pueden reasignarle el nombre a otra persona. Número dos, pueden cambiar el resolutor. Tres, pueden crear subdominios. Aquí ven la estructura jerárquica.

En cuanto a los resolutores, su responsabilidad es responder preguntas sobre un nombre. Por ejemplo, ¿qué dirección está asociada con este nombre? ¿Qué registro de IFPS está asociado con este nombre? La resolución de nombres en ENS es muy sencilla. El usuario hace una consulta al registro preguntando cuál es el resolutor para, por ejemplo, foo.eth. El registro dice: "Es un 1234" y después se le pregunta al resolutor: "¿Cuál es la dirección de foo.eth?" Y el resolutor contesta: "Es XX", lo que fuera. O X2345.

Hicimos un lanzamiento preliminar de ENS. Duró ocho semanas. En estas ocho semanas gradualmente fuimos lanzando una serie de nombres populares a los usuarios a través de un proceso de subastas. Los fuimos lanzando en forma gradual para no aumentar demasiado los costos de las transacciones. Terminamos con este proceso a fines de julio y en este proceso se subastaron alrededor de 150.000 nombres. Se logró un nivel de actividad muy interesante. Además, durante este proceso, se depositaron 168.595 ether, que son como 55 millones de dólares.

Si una persona obtiene un nombre, el ether se deposita, se bloquea por un año por lo menos. Después se le devuelve a la persona.

Entonces la adopción de los clientes de ENS es buena. Se han aceptado diferentes ENS y esperamos que más clientes sigan utilizando ENS como tecnología a medida que esta madure. También organizamos nuestro primer taller DNS en agosto, en 2017 con 27 participantes. En este taller cubrimos muchos de los temas que se están tratando en la ICANN. Resolución de disputas, diseño de registrador permanente, cómo garantizar y asegurar los subdominios y cómo integrar con el sistema existente DNS en la actualidad. Logramos hacer una integración de DNS a través de DNSSEC. Aquí pueden ver la cadena. Empezamos con el hash de la clave de DNS. Después se verifica la clave del DNS, etc. hasta llegar a un registro que vemos en el último casillero. Para aquellos de ustedes que son de DNSSEC, esto es lo mismo solo que en la última parte, en lugar de asegurar un registro, estamos asegurando un registro de texto con el valor de la dirección de Ethereum.

¿Cómo vamos a avanzar con este proceso? El usuario debe ser aprobado. Se comunica con la base de datos Oracle y le informa al registrador que es el dueño de este subdominio. El registrador después consulta Oracle preguntando si el usuario demostró o probó su identidad. Oracle contesta sí o no y en base a eso el

registrador registra el subdominio en el sistema de ENS. Hemos estado trabajando en esto. Lo estamos probando y en teoría esto se puede hacer para cualquier TLD que permita trabajar con hashing. Hay tres tipos de TLD hoy en día que permiten esto. Muchas gracias. Por favor, sigan conectados para escuchar más novedades sobre ENS. No sé si hay alguna pregunta.

DAVID CONRAD: Tenemos tiempo para preguntas sobre Ethereum. Yo tengo una pregunta. Es la siguiente. Obviamente esto tiene que ver con .ETH. Quiero saber qué piensan hacer a futuro en relación con el dominio de alto nivel o la identificación que utilizamos para ese tipo de dominios.

LEONARD TAN: Entendemos que .ETH es el código de país para Etiopía así que no lo vamos a poder usar pero estamos intercambiando ideas. En este momento estamos pensando en la integración con los sistemas ya existentes y en probar si ENS es funcional y después vamos a ver qué pasa.

DAVID CONRAD: Para aclarar esto, .ETH, los códigos de tres letras no están reservados. El hecho de que sean las tres letras que pueden representar a Etiopía no significa necesariamente que ya esté

reservado para Etiopía. Si la próxima ronda de gTLD tiene lugar, quizá ustedes podrían participar o no. John.

JOHN LEVINE: Gracias. Tengo un tema de seguridad que me preocupa porque las cadenas de bloques son tan seguras como los mineros. Los bitcoin están controlados por grandes pools de mining en China. No sabemos para qué lo usan. ¿Sabe usted quién hace el mining para Ethereum? ¿Podemos creer que no son pools de mineros que se pusieron de acuerdo?

LEONARD TAN: Primero voy a hablar de bitcoin. A pesar de que la mayoría de los mineros están en China, históricamente todos los mineros siempre se mueven por incentivos. Por eso funcionan las cadenas de bloques, porque los mineros responden a los incentivos.

JOHN LEVINE: [inaudible]

LEONARD TAN: Pero aun así, los mineros van a hacer aquello para lo que fueron incentivos a hacer.

JOHN LEVINE: En lugar de discutir si es posible, quisiera saber si saben quiénes son los mineros o si están asumiendo que siempre va a haber suficientes mineros y habrá suficientes grupos como para que no nos preocupemos de que un grupo asuma todo el control de estas cadenas de bloques.

LEONARD TAN: Este es nuestro objetivo, tener un sistema distribuido para evitar que se creen grupos de minería especializada. La idea es tener un entorno distribuido pero en cuanto a su pregunta, si podemos trabajar para que las personas no se reúnan y trabajen en grupos, no sé si podemos hacer algo. Podemos crear un sistema para que todo el mundo pueda hacer minería en igualdad de condiciones pero en cuanto a impedir que se agrupen entre sí, bueno, eso ya es difícil.

DAVID CONRAD: ¿Hay alguna otra pregunta? Paul.

PAUL WOUTERS: Soy Paul, del IETF. Tengo una pregunta. Supongamos que IETF recibe el dominio IETF en este sistema de nombres y pagamos nuestros aranceles por un par de años. Todo el mundo usa el sitio. Después, en algún momento nos olvidamos de pagar y el dominio vuelve a caer a la lista de dominios disponibles, otra

persona lo registra, no sabemos quién es ni dónde está. Voy a un sistema judicial y alguien me dice que tengo derecho a tener esta marca comercial y que me tienen que devolver este dominio. ¿Hay forma de que yo pueda recuperar este dominio?

LEONARD TAN: En la actualidad, la respuesta sería que pueden volver a recuperarlo pero se necesita un consenso de cuatro de las siete personas que integran el grupo que decide. Podrían recuperar su marca comercial. Es difícil pero posible.

DAVID CONRAD: Okey. Una pregunta más y pasamos a la próxima presentación.

JORDI PAILLISSE: Hola. Quisiera señalar que con respecto al debate de mining hay aproximaciones a mining que no requieren mineros especiales para este proceso. Toman un abordaje diferente y utilizan el valor que está dentro de la cadena de bloques para generar los nuevos bloques. Es una aproximación que podría utilizarse. Gracias.

DAVID CONRAD: Gracias. Gracias, Leonard, por su comentario. Pasamos ahora a Michael Palage y Pindar Wong, quienes van a estar a cargo de la próxima presentación. ¿Podemos cambiar las diapositivas?

PINDAR WONG: Gracias. Michael y yo somos voluntarios en el grupo de interés de especial de cadenas de bloques. Estamos aquí porque hace dos meses estábamos hablando acerca de la evolución de esta joven tecnología llamada cadena de bloques. De hecho, ayer no fue necesariamente Halloween. Fue el noveno aniversario de la publicación del documento sobre bitcoin. Nos interesa este desarrollo de los sistemas de nombres como el que acaban de ver. El ENS es una de estas cadenas de bloques. Ayer había 1.234 cadenas de bloques. Ahora hay 1.244 cadenas de bloques. Algo está pasando y cada uno va a enfrentar problemas similares. Tenemos estas direcciones de 34 caracteres que tienen una aleatoriedad esencial. Creo que la comparación general que nos gustaría hacer hoy a través del documento que acabamos de publicar es que hay algo que está pasando aquí que requiere que los nombres y los gobiernos estén involucrados. En este caso, es un mapeo de clave pública y nombres. Quisiéramos hacer una presentación de esto.

En primer lugar quiero agradecerle a Michael personalmente por plantearme este tema. Originalmente pensé que era un riesgo

con un horizonte a largo plazo pero desde entonces hemos empezado este debate. Las cosas han empezado a cambiar y también quisiera hablar desde el punto de vista descentralizado. Tratamos de establecer las oportunidades y los riesgos en el horizonte y el nuevo grupo del comité técnico de la junta el viernes. Ayer ampliamos los sistemas de nombres de cadena de bloques e ID descentralizados. Hoy querríamos hablar acerca de por qué esto es pertinente para la ICANN hablando acerca de la evolución y la revolución.

Como ustedes saben, la Internet es flexible. El tema con respecto a la innovación es que pasan cosas, cosas como bitcoin. En este caso, lo disruptivo está perturbando. Esta tecnología de cadena de bloque proviene del borde. Bitcoin no salió de los procesos estándares que ya conocíamos. Primero salió como código de un documento técnico. Lo que quiero señalar es que yo creo que a la junta directiva y a este comité este tema les debería interesar porque podría cambiar algunos supuestos como una única raíz global, por ejemplo. Lo que es más importante, podría llevar a cambios en la estructura del mercado. Obviamente, tenemos todo el ecosistema del DNS pero lo que más me preocupa a mí en este momento, y estoy utilizando el ejemplo de hoy de 10 cadenas de bloque más que ayer, es la tasa de innovación y la velocidad de adopción en este espacio.

Los últimos dos puntos de contacto que utilizamos, por ejemplo, para el ENS es lo que acaba de escuchar. La idea es que esto funcione con el DNS existente pero elegimos otro ejemplo de algo que está totalmente fuera del sistema del DNS. Se llama Blockstack. También tenemos ya colisiones de nombres dentro del sistema de nombres de cadena de bloque con nombre diferente. Yo estoy involucrado en esto. Ayer hablamos acerca de los identificadores descentralizados que son los procesos estándares con los que estamos familiarizados. En este caso, el grupo W3C. Hay innovación, tanto dentro de los foros tradicionales, como seguramente todos sabremos en términos de riesgos y oportunidades en el horizonte pero también podría haber otros sistemas como bitcoin que están fuera del radar y aquí en este documento que hicimos circular planteamos esta oportunidad para que todo el mundo esté informado al respecto y para que los nuevos dirigentes también estén informados.

El supuesto era el mismo supuesto que existía antes de que surgiera Internet. Si uno entendía este supuesto, podría ganar mucho dinero a través de los ISP que era el tema de que distancia es igual a costo. Dependiendo de la distancia, variaba el costo de un llamado telefónico por ejemplo. Ahora tenemos videoconferencia y no nos importa. PreICANN tenemos gobernanza igual a tratados bilaterales. PostICANN tenemos gobernanza global, múltiples partes interesadas. Bitcoin es un

ejemplo específico en donde los datos específicamente en este caso pueden ser iguales a dinero. Datos igual a dinero.

Lo que yo quiero sostener es que pre cadena de bloques, que es algo que nos podría preocupar, presupone que centralizado es igual a seguro. Hacemos un firewall que sea lo suficientemente alto y quizá las cadenas de bloques estén descentralizadas y sean más robustas, más seguras y en este caso potencialmente persistentes con los identificadores descentralizados.

Ese es el punto que quiero señalar. El proceso de desarrollo, por ejemplo Ethereum, la reunión de desarrollo tiene lugar hoy en México. Ellos tienen un proceso de desarrollo que se llama EIP y Bitcoin es similar. Tiene algunas propuestas. Ellos también tienen una conferencia que va a comenzar mañana en Stanford. Ya que estamos, David, esto imitaba a APRICOT cuando fue creada.

Ayer hablamos acerca de los reclamos verificables, el rebooteo de la web de confianza y de los materiales de la raíz. Está el grupo que es el grupo de credenciales que está dentro del proceso de W3C y se reúnen creo que el lunes de la semana que viene.

También queremos demostrar la variedad de foros en los que están teniendo lugar estos debates. Yo diría que además del grupo de credenciales, los demás no forman parte de los

procesos estándares. Queremos asegurarnos de que sepan que existen estos grupos que están fuera del proceso normal de creación de estándares y están trabajando con ritmo de innovación muy rápida. Hay dos que podrían interesarles especialmente. Son cadenas de bloques públicos. Ya escucharon hablar de Ethereum, de bitcoin. Hay otro IoT que se ocupa del Internet de las cosas pero podemos ver los distintos modelos de gobernanza que podrían darnos una oportunidad para que la ICANN considerara su papel considerando alguno de los temas que identificamos en nuestro documento. Habiendo dicho esto le voy a dar la palabra a Michael, quien va a hablar acerca del documento. Ustedes tienen un resumen de este documento frente a ustedes.

MICHAEL PALAGE: Muchas gracias. Tal como dijo Pindar, en ISOC BSIG, una de las iniciativas que estamos tratando de llevar a cabo es generar conciencia acerca de estas nuevas tecnologías y su impacto potencial sobre la ICANN. La ICANN debería ser felicitada por contactarse en Copenhague y haber estado en la sesión de identificadores. Ahora tenemos Ethereum, ENS y la tercera tecnología importante que cubrimos en el documento que hicimos circular y que publicaremos formalmente a fines de este mes es Blockstack.

Cada una de estas tres tecnologías tiene un impacto potencial diferente sobre la ICANN. Tal como lo señala el título, puede ser en el sentido de una evolución o de una revolución. Esta es una de las razones por las cuales tratamos de plantear este tema. Otra de las cosas que hicimos en este trabajo fue analizar qué están haciendo los miembros de la comunidad, específicamente con respecto a la solicitud de patentes. Una de las cosas que me llamó la atención en mi investigación fue que Verisign solicitó tres patentes en Estados Unidos a principios de este año. Esto podría tener un impacto potencial. El título específico de esas patentes es "Anclajes de confianza de DNS para objetos que están fuera del DNS". Luego hay una referencia específica al uso de registros públicos y cadenas de bloques.

Además, otro miembro de la comunidad de la ICANN, Bill Manning, también solicitó una patente. Esto es importante. Esto está pasando. Esto solo es nuestro análisis inicial relacionado con las solicitudes de patentes en los Estados Unidos. En las próximas semanas, ese artículo será sometido a una organización de pares y se verá si hubo aumentos con respecto a esta tecnología a nivel internacional.

Lo que también señala nuestra investigación es que hay una serie de otros foros internacionales que trabajan activamente en este campo. Tal como dijo Pindar, el W3C junto con sus reclamos verificables, ISO TC307 con respecto a la estandarización de la

cadena de bloques y nuestros colegas de la UIT también han trabajado activamente en el SG17 y SG20. El propósito de este documento es no dirigir a la ICANN para que haga algo sino simplemente brindarles esta información. Yo tuve el honor de trabajar con Tricia Drakes. Ella siempre habla de un liderazgo de líderes con información. La idea es que tengamos sólidos líderes y que la ICANN sepa que existe esta tecnología. Sabemos que ustedes tienen muchos temas que cubrir pero nos parece que esto es algo a lo que tendrían que prestar atención. Una vez más, esperamos poder publicar este trabajo a fin de mes.

PINDAR WONG: Ayer a la noche tuvimos una teleconferencia. Hablamos con el [BC] acerca de este informe de seis páginas. Una vez más, es una versión preliminar. Luego haremos comentarios. Es solo para brindar un marco. Quizá esté totalmente equivocado. No lo sabemos. Por lo menos es un intento por dar un marco y un ejemplo del rango de actividades e iniciativas que están teniendo lugar. Desde aquellas que están en función hasta aquellas que no funcionan. Una vez más, la idea es que estos identificadores descentralizados son persistentes. Utilizan URN, entonces muchos de los temas que mencionamos antes acerca de la persistencia podrían encontrarse allí.

La pregunta entonces es si en el consorcio que yo inicié por lo menos podemos trabajar sobre esta noción de marcas registradas, marcas comerciales. La pregunta es: Cuando tenemos una de estas direcciones para bitcoin o lo que sea, ¿cómo sabemos que se mapea si la ICANN tiene una billetera electrónica, por ejemplo? ¿Cómo puedo estar seguro de que esa dirección realmente se mapee con la ICANN o Coca-Cola o lo que fuera? Estamos tratando de ir un paso más allá y pensar qué podría reforzar las fortalezas de la ICANN y de la comunidad. Ustedes ya hicieron tanto en términos del proceso ADR, la familiaridad con los IP. Esto va a ser importante si ya estamos lidiando con miles de cadenas de bloques potencialmente. Habrá violación de derechos de marca registrada cuando la gente registre este tipo de nombres. Esto no solamente no va a ser bueno para esa industria sino que potencialmente podría distraer a algunos miembros de la comunidad de la ICANN para que participen en otros foros justo en un momento en el que tenemos la oportunidad de avanzar con la ICANN. ¿Alguien tiene alguna pregunta?

MICAHEL PALAGE: Creo que nos quedan dos minutos de nuestros 15 minutos así que quiero agregar algo. Quiero mostrarles cómo está surgiendo esta tecnología. Él señaló antes que se registraron 180.000 nombres en el DNS. Si comparamos eso con la cantidad actual

de nuevos gTLD aprobados en 2012, estaría entre los primeros 50 de los casi 1.000. Para mí, eso es un punto de datos importantes que no deberíamos ignorar. Otro punto de dato importante es que, si se fijan en el mercado total de nombres de dominio, los nombres de dominio registrados, creo que la valoración actual es 55 millones.

Históricamente, si miramos hacia atrás, vemos que esto es equivalente aproximadamente a 1998 cuando tuvimos el documento técnico y el documento verde. En ese momento había unos tres millones de nombres de dominio registrados en todo el mundo a 35 dólares por año. Creo entonces que es importante ver la historia a medida que avanzamos. Buscar paralelos. Gracias. Con todo gusto vamos a responder sus preguntas.

DAVID CONRAD: ¿Alguien tiene alguna pregunta para Michael o para Pindar? Wendy.

WENDY SELTZER: Gracias. Gracias por su participación. Usted mencionó los grupos de W3C. W3C utiliza grupos de la comunidad como un entorno de laboratorio similar para aquellas cosas que nosotros observamos y exploramos. ¿Hay algo estándar que esté

surgiendo de este trabajo? Me refiero al grupo de cadena de bloques de la comunidad W3C. Hay un grupo de trabajo que está considerando un vocabulario estándar para afirmaciones acerca de atributos. Nosotros también estuvimos analizando esto. Hay mucho entusiasmo, mucho interés. A nivel de los datos, estamos viendo cuando hay interés en estandarizar algunos componentes por encima de eso. Nos encantaría y vamos a tratar de continuar a partir de ahí.

PINDAR WONG: Gran parte del debate se concentra en cadena de bloques, prueba de concepto, prueba de funcionamiento, etc. Hay una gran generalización aquí pero los modelos de seguridad de los sistemas están incompletos. Están incompletos porque hay una capa de seguridad que todavía no entendemos totalmente. Ahora estamos trabajando en una red con 22 universidades para tratar de resolver esto. Tenemos estos tokens que potencialmente tienen un valor económico. Ethereum es un ejemplo. La parte económica, el valor económico del token afecta a la toma de decisiones de la gente, ya sea de forma especulativa, para retenerlo, etc.

No se trata claramente de la tecnología únicamente. También hay un incentivo económico que conduce a comportamientos extraños. Cuando esto se convierte en algo más generalizado,

cuando queremos que una empresa tome estos activos digitales como valor en una billetera, entonces van a querer hacer cumplirlo, quieren asegurarse de que el público crea que la billetera les pertenece.

Nosotros en este tiempo trabajamos concentrándonos en un área. Cómo nos aseguramos de que los identificadores de entidades legales funcionen con las corporaciones. Cómo hacemos ese mapeo entre eso y la identidad digital de esos sistemas para cualquiera de estas cadenas de bloques porque no sabemos qué cadena de bloques será la cadena de bloques. Aquí la oportunidad para la ICANN consiste en considerar en qué medida va a participar en otros foros y/o qué relación va a tener cuando llegue el DNS, qué modalidad de participación va a considerar, ¿va a hacer proactiva, reactiva o una combinación? Creo que estamos en una etapa inicial del proceso. Podemos adelantarnos si ven que hay una oportunidad, más que una amenaza.

DAVID CONRAD: Gracias. Ahora vamos a pasar a la Última presentación de esta tarde que estará a cargo de nuestro estimado presidente por 24 horas más sobre el proceso de actualización de la zona raíz a prueba de acceso no autorizado.

CHERINE CHALABY: Si no les importa, lo que escucho decir allí, en ese lado, es que la tecnología de DNS tal como la vemos no va a sobrevivir. Es lo que están diciendo. O se va a mejorar o se va a remplazar por esta nueva tecnología. ¿Está de acuerdo con esto como director de tecnología o no?

DAVID CONRAD: Siempre fui de la opinión de que nada queda igual. La tecnología evolucionará o desaparecerá. Los vectores del cambio todavía no los veo claramente. Hay muchas cosas fascinantes que están sucediendo en el mundo de cadenas de bloques. Ahora, si esto se aplica directamente o no, hay muchos argumentos que sugieren que esto es posible pero yo tengo ciertas dudas. Simplemente porque no entiendo completamente la tecnología como para tener una opinión certera y con confianza. Este es uno de los motivos por los cuales estoy incentivando a mi equipo a investigar la tecnología de cadenas de bloques para entender con sus consecuencias y para ver cómo esto va a impactar sobre el ecosistema de la ICANN y más allá de esto, sobre el sistema de identificadores del cual depende Internet. Pindar, ¿qué opina usted? ¿Cree usted que la cadena de bloques va a remplazar al DNS?

PINDAR WONG: El sistema de escala es importante. Estos sistemas no escalan bien. Empezamos a escalar un grupo de nosotros los bitcoin o el protocolo bitcoin y tuvimos éxito por dos años y medio. Ahora estamos manejando en lugar de tres o cuatro transacciones por segundo, podemos hacer 40.000 transacciones por segundo. En la capa dos, el prototipo ahora funciona en la capa de cadenas de bloque con 100.000 o más. El tema es que cuando cambian los supuestos, cambia la estructura del mercado. A mí lo que me interesa más es la comunidad técnica y no la tecnología específica. La comunidad de bitcoin, yo soy maximalista de bitcoin porque esa comunidad es sorprendente, maravillosa. Yo soy la persona más tonta aquí, la que menos sabe, así que estoy en el lugar adecuado.

¿Qué va a pasar con esto? No sé pero algo está pasando y para que esa tecnología tenga éxito, debe ser más utilizable. En general, hablamos de nombres y esto en sí mismo puede ser un error cuando hablamos de computadoras sin pantalla pero quién sabe. Por el momento tiene que ser algo más usable. Estamos utilizando códigos QR. DNS es el primer ejemplo que es fácil de entender pero transacciones máquina-máquina, necesitan usar el DNS. ¿De qué estamos hablando exactamente? Si el supuesto es que hay una sola ruta única final y definitiva, si pensamos en un mundo donde hay certeza estadística y eso alcanza, eso hace desaparecer muchos supuestos. Creo que lo

más importante ahora es no involucrarse demasiado con la tecnología. Solo hay que ver cuáles son los supuestos y cómo esto afecta los supuestos de la ICANN. Si los supuestos que utilizamos en el ADN de la ICANN cambian, eso será lo importante. Realmente aliento a la ICANN a que desarrolle su propia estrategia de blockchain como lo hacen todos. Todos están tratando de definir su estrategia de cadena de bloques.

JAY DALEY: Gracias. Recordando la respuesta que dio Cherine, debemos separar DNS del negocio de registro. Las cadenas de bloques pueden hacer cambios importantes en el negocio de los registros. No sé si tiene la posibilidad de hacer cambios importantes en el DNS.

DAVID CONRAD: Dr. Crocker, usted tiene la palabra.

STEVE CROCKER: En comparación, el tema del que voy a hablar se ocupa de un problema muy simple con la tecnología existente sin tratar de incorporar nuevos paradigmas que afecten todo el ecosistema. En realidad es bastante retrógrado en comparación con todos los temas avanzados que se han tratado. No hay reconocimiento de voz en estos equipos.

Bien. Este es un trabajo que surgió de conversaciones que tuve que soportar durante muchos años. Todo esto es cierto. Nos sentamos con funcionarios importantes de diferentes gobiernos a discutir y a hablar. Hablamos como si esto fuera una amenaza seria que el gobierno de los Estados Unidos o la ICANN o alguna combinación de ambos o alguna versión equivalente pudiera hacer un cambio abrupto. El más sencillo sería sacar su registro de la raíz. El código de país, XQ, lo que fuera, desaparece de repente. Entonces las referencias en la raíz no devuelven nada o dicen: "No existe". Ellos piensan que esto podría suceder en un periodo durante el cual haya tensión política muy grave. Eso sería un movimiento ofensivo y les preocupa.

Lo que hice muchas veces en esos casos es explicar por qué eso no va a suceder. Todo el sistema de frenos y equilibrios, cuáles son los procesos que tenemos, etc. Además, que si esto sucediera, el impacto sería relativamente lento e incremental. Tenemos 48 horas para que se modifiquen los registros en la raíz. Habría una degradación del 2% por hora en la memoria caché. Sin embargo, la noticia de que esto pasó se difundiría 15 veces más rápido que la velocidad de la luz por todo el mundo. No tan rápido pero entienden lo que quiero decir. Los administradores del sistema y los boyscouts tratarían de resolver el problema encontrando otras formas de llegar. Lo que harían seguramente es diferente y mejor que lo que pensaría hacer cualquier

funcionario del gobierno de los Estados Unidos, no en forma directa sino indirecta, sería sugerir que si algún gobierno quisiera impulsar a los Estados Unidos a sentirse muy avergonzado, podrían obligarnos a hacer esto de alguna manera porque esto realmente afectaría a la credibilidad de la ICANN y al gobierno de los Estados Unidos.

Sin embargo, he logrado entender que se habla mucho de esto y las personas que hablan de esto entienden exactamente lo que yo acabo de decir. No son tontos, no les falta educación pero como se puede pensar en el problema, se transforma en algo que podemos utilizar para discutir. Podemos decir que es un problema. Podemos hablar muchísimo al respecto. Es posible contrarrestar esto, no a través de actividades políticas ni con temas de organización sino realmente a través de una protección técnica de manera que sea absolutamente imposible que eso suceda.

Les voy a dar el contexto ahora. Como dije antes, el escenario de pesadilla es que se saca un nombre de la raíz en forma abrupta. Continuamente hacemos cambios en la raíz. Hay un proceso para eso. No es tan fácil como decir: “Nunca vamos a hacer un cambio en la raíz”. La idea es que el proceso de cambio involucre a la parte afectada que debería estar de acuerdo. Si no está de acuerdo, no se hace ningún cambio. Esto no alcanza tampoco porque habrá casos en los cuales este grupo no puede estar de

acuerdo, no quiere estar de acuerdo e igual hay que hacer el cambio. Esta es la descripción general.

Ahora vamos un poco más en detalle. La motivación es, como dije, la que ya mencioné. La pregunta sería: ¿Es posible definir y preparar un sistema que impida que se dé este escenario de pesadilla? La respuesta es sí. El concepto básico está basado en un sistema sellado que no permita el acceso no autorizado. Tenemos un sistema actual en DNSSEC. Si se trata de acceder en forma no autorizada, si tenemos una clave privada, la clave se anula automáticamente. Eso hace que el sistema sea inoperable pero no desactiva la clave privada. Es decir, el sistema es inoperable y ya no se pueden hacer cambios. Para lograr un punto intermedio entre hacer cambios inadecuados y no poder hacer ningún cambio, sería lograr un equilibrio entre falsos positivos y falsos negativos o, en otros términos, errores tipo 1 o errores tipo 2.

En este caso, como en muchas otras situaciones de la vida real, hay una gran diferencia en el impacto de un tipo de error o de otro tipo de error. En este entorno, cometer un error por hacer un cambio no adecuado es mucho peor que no poder hacer ningún cambio. Tenemos demoras incorporadas al sistema. No sabemos cuánto tiempo va a llevar. Ahora sí se puede con los acuerdos de nivel de servicio pero durante mucho tiempo había

bastante flexibilidad en cuanto al tiempo que llevaba hacer un cambio. Ese tipo de equilibrio funciona muy bien.

El concepto aquí es un sistema sellado al cual no se puede acceder sin autorización. Nosotros tenemos un control dividido. Tenemos una base de datos mantenida por la PTI y por IANA y una mantenida por Verisign y hay comunicación entre ambas. Todo esto debe estar sincronizado. Es posible crear un sistema sellado que incorpore todo esto. Es un poco más fácil si lo ponemos todo en un lugar pero no es imposible hacerlo si hay dos organizaciones. Además, podemos pensar en la zona de raíz como que está dividida en pequeñas partes con una parte asignada a cada dominio de alto nivel. Hay un poco de información para cada dominio de alto nivel en cada uno de esos sectores. La información principal asociada con todos los dominios es cuál es el conjunto de servidores de nombres. Con DNSSEC también tenemos las claves, los registros DS asociados. Hay más detalles y es un poco más complejo, cuando hablamos de los registros de direcciones que son relevantes.

Hablaremos también un poco más sobre cómo se manejan los registros para servidores raíz y también los registros autoritativos. Estos temas se pueden resolver fácilmente. Son temas más detallados que no voy a tratar en esta sesión.

El próximo concepto que subrayé varias veces ya es que no se debe hacer ningún cambio en la parte de la raíz de los TLD sin la aprobación de los TLD, de los propietarios o de los operadores. A veces un operador de TLD dice: “Quiero hacer un cambio” y no están contentos porque el cambio no se da inmediatamente o no se da en absoluto. Este es un problema diferente. También podríamos decir que es importante tener un sistema robusto pero igual pueden surgir otros aspectos que hay que tener en cuenta.

Si lo pensamos así, sin hablar de lo que sería tener un token de hardware, eso se podría hacer con el software pero supongamos que tenemos un token de hardware, un dispositivo que le damos a un operador de TLD, que debe utilizar ese dispositivo para autenticar y autorizar un cambio futuro. Si no lo hace, el cambio no se puede realizar. ¿Cómo lo reciben en primer lugar y cómo hacemos la asociación entre el operador y el dispositivo? Este es un proceso diferente que exige separar esta idea de que no se puede hacer ningún cambio sin la aprobación. Necesitamos un proceso un poco más complejo. Tenemos ceremonias de clave y otros procesos similares. Tenemos toda una serie de personas que se ponen de acuerdo en que esto es lo que debe hacerse y estas personas son suficientemente independientes como para evitar colisiones y otro tipo de presiones y para que todo el proceso sea lento, deliberado, documentado y visible.

Este es uno de los abordajes que hay que usar para estos procesos lentos. Además, si estamos pensando en una reasignación hostil, este sería otro caso. Supongamos que alguien pierde esta clave, o se quema esta clave. Son las cosas que pueden pasar. La solución general en todos estos casos sería pasar por un proceso lento, laborioso, muy visible y documentado. Este es el control político a través de múltiples partes.

El próximo punto sería… Bueno, no todo el mundo va a poder hacer esto ni todo junto. Solo tenemos 1.500 operadores de TLD en la actualidad. 10 van a estar listos hoy y los otros 1.490 van a llevar más tiempo. Los últimos 1.000 van a llevar 2 o 10 años, lo que fuera. Es un proceso de transición. En todo diseño hay que estar preparado para operar con el sistema actual y el nuevo sistema. Esto estaría bien. No hay un problema aquí. Podríamos pensar en modificar completamente el sistema y después utilizar nuestros dispositivos para cada operador de TLD listo para que lo use en su momento. Los que están listos para empezar a usarlo se lo envían. Los que no, ustedes hacen el proceso en su nombre y no se notaría la diferencia.

Este es el proceso de actualización de la zona raíz. Entran cambios desde el operador de TLD. Lo que vemos a la izquierda pasan a la función de la IANA, que es la PTI, que valida la solicitud. Dice: “Está aceptada”. La envía a Verisign que es el

cuadrado que está abajo y de este diagrama hace dos cosas. Edita la base de datos y crea una zona raíz. No incluí a propósito la generación de claves y la firma que eso haría más complejo este diagrama. Después lo pasa al proceso de distribución dos veces por día. Queda una nueva versión de la zona raíz que está disponible para los 13 operadores de los servidores de zona raíz. Así se dan los cambios de los que hablamos.

Además, según el nuevo cambio, la columna del medio estaría en un sistema sellado, hermético, o si hay dos grupos que operan dentro de este sistema, serían dos sistemas de hardware. Ambos son a prueba de acceso no autorizado y tendrían un protocolo robusto que los conecta entre sí. Para repetir, hay dos clases de transacciones. Las comunes, con los cambios comunes en los registros DNS y la clave de DNS, y aquellos que pasan por la vía rápida hasta que el operador dice. “Quiero este cambio, esta es mi autorización para solicitar el cambio” y ese cambio puede ser autorizado o no pero no se puede hacer en forma no autorizada, sin autorización del operador. Los cambios más importantes son cambios en el control, etc. y exigen este proceso más complejo.

Este es otro diagrama de un cambio regular, común. Lo que deberíamos tener aquí no lo pude expresar muy bien pero piensen que arriba tenemos una mesa de conferencias alrededor de las cuales están sentadas muchas personas que desarrollan procesos. Es muy parecido a la forma en que hacemos las

ceremonias de clave hoy en día con representantes confiables de la comunidad. Básicamente aquí repetimos lo que ya dije. El organismo de supervisión sería un grupo de personas de confianza.

Si queremos explorar esto, los próximos pasos serían presentar un diseño conceptual, documentarlo, compartirlo y si podemos dividir el trabajo en tres vías de trabajo paralelas, explicando cuál sería el proceso, podríamos crear prototipos de interacción entre el operador de TLD y el sistema. Podríamos crear un prototipo de cómo funcionaría el sistema. Estos tres pasos podrían hacerse en cualquier orden a fin de poder recabar más información. Creo que esta es la última diapositiva. Este es el concepto. Hace bastante tiempo que estoy pensando y trabajando en esto. No me acuerdo de cuándo empecé a trabajar en esto pero dejé de hablar de esto completamente y lo dejé de lado cuando empezó el proceso de transición porque pensé que nos iba a distraer del tema e iba a causar confusión. Ahora ya pasó la transición así que aquí estamos nuevamente. Muchas gracias.

DAVID CONRAD: Antes de pasar a las preguntas quería señalar que mi equipo piensa solicitar dos tipos de cambios. Uno es un cambio que implica una evolución para mejorar el sistema y el otro es un

abordaje revolucionario que reestructura la forma en que hacemos las cosas. Una de las ideas era incorporar esta idea de un sistema a prueba de accesos no autorizados en el sistema revolucionario. Estamos pensando, como dije, en lanzar un llamado a la presentación de propuestas. No sé si hay preguntas. Espero que no haya muchas preguntas, salvo que queramos saltearnos el cóctel. Kathy no estaría muy contenta con esto. Rod.

ROD RASMUSSEN: Es muy interesante este abordaje. Me pregunto lo siguiente. Esto es administración de la zona raíz. Yo diría que los TLD .MARCA también estarían interesados en esto potencialmente. Obviamente con diferente modelo de gobernanza pero por qué detenernos en la raíz.

STEVE CROCKER: Sí. Precisamente. La misma tecnología puede aplicarse a todos los niveles obviamente. Entonces sí. Punto.

DAVE PISCITELLO: El único modelo de amenaza que instiga esto es que la gente se preocupe por si algo no funcione. A mí me gustaría ver un modelo de amenazas y un análisis de costo-beneficio para entender mejor cuál es el resultado final de cambiar lo que

tenemos y cuáles son las amenazas que mitigamos y que no podemos mitigar hoy con el modelo existente porque no veo las amenazas tan obvias como quizá alguien que diga: "Estados Unidos va a tomar represalias".

STEVE CROCKER: Traté de decirlo al principio. Si uno está sentado cerca del centro del mundo, como usted y yo, a nosotros nos parece que esto es absolutamente ridículo y que nadie debería preocuparse por esta clase de cambios. Pero si nos vamos a lugares más lejanos, de pronto parece que: "Dios mío, estamos en riesgo. Todo el país y toda la economía van a quedar destruidas de un día para el otro". Ese es el modelo de amenazas.

DAVID CONRAD: ¿Una última pregunta?

LARS-JOHAN LIMAN: ¿Esto evita la negación del servicio?

STEVE CROCKER: No. Traté de mencionar esto antes. Tuve una conversación interesante hace varios años con un operador importante de TLD. Le pregunté cuánto tiempo le llevaba hacer un cambio. Cuánto tiempo debería tomarle hacer un cambio en sus

operaciones con un nuevo nombre. Me dijo: “Máximo, 48 horas”. En contraposición a lo que pasa con .COM, donde uno puede hacer eso en pocos segundos o en un minuto. Yo dije: “¿Cuánto tiempo planifican?” Entre seis y ocho semanas. Es así. Es real. En esa época lo que me expresaba es que hay un pedido pero ellos no están seguros de que esto se mantenga. Puede desaparecer. Hoy en día estamos en mucha mejor situación. De todas formas, yo creo que los operadores de TLD van a tener que hacer cambios en la configuración del servidor de nombres y no están en la posición donde tienen que hacerlo instantáneamente. Si reciben una solicitud y no ocurre, entonces hay que escalarlo y hay procesos de escalamiento normal. Su caracterización de que esto no ocurre de hecho es el comienzo de un proceso donde no ocurre ahora pero pasa por un proceso más extensivo y se convierte en una demora en lugar de en una negación absoluta, a menos que haya una razón para descartarlo totalmente.

LARS-JOHAN LIMAN: Yo me refiero a esto por una razón política.

STEVE CROCKER: Si hay una razón política, entonces tenemos que resolverlo a nivel político.

DAVID CONRAD: Habiendo dicho esto, llegamos a la parte de “Otros asuntos”. El único otro asunto que tenemos es que todos los interesados en el cóctel deberían ir ahora a la entrada principal. Habrá ómnibus que nos llevarán al lugar… No lo voy a pronunciar porque seguramente lo voy a pronunciar mal. Nos van a llevar a un lugar de observación, en un lugar precioso. Seguramente vieron fotos en revistas hermosas y revistas de viajes. Muchas gracias a todos. Nos volvemos a ver en Puerto Rico.

[FIN DE LA TRANSCRIPCIÓN]