COPENHAGUE - Reunión conjunta: Junta Directiva de la ICANN y Grupo de Expertos Técnicos (TEG)
Miércoles, 15 de marzo de 2017 – 17:00 a 18:30 CET
ICANN58 | Copenhague, Dinamarca

STEVE CONTE: Si alguien está buscando al grupo de aceptación universal, se trasladó de esta sala a la sala B5.1. No es que no le queramos aquí, pero si está buscando algo distinto a la sesión del TEG, y es la aceptación universal, está en la sala B5.1. Y ahora quiero jugar a la batalla naval.

DAVID CONRAD: Qué... oh, guau. La fiesta puede comenzar. Aquí está Jonne.

>> (Fuera del micrófono.)

DAVID CONRAD: En realidad, aún estamos haciendo un pequeño malabarismo logístico en este momento. Steve y Lousewies dicen que están en camino, así que estarán aquí de un momento a otro. Intentamos hacer malabares con algunas diapositivas ahora.

>> (Fuera del micrófono.)

DAVID CONRAD: Sí, en realidad podemos comenzar con algunas presentaciones, si así lo desean. Para el contexto, esta es la Junta Directiva contra los expertos técnicos, el partido de jaula. Bien. Tal vez no.

Esta es la... no sé, reunión número algo del Grupo de Expertos Técnicos. Y se creó para permitir a los expertos técnicos brindar aportes a la Junta Directiva. No brindamos asesoramiento, brindamos aportes. Es... originalmente era una sesión cerrada, pero desde entonces la hemos abierto y hemos dado la bienvenida, ya saben, a cualquiera que esté interesado en participar en cosas relativas a los fanáticos de las computadoras.

Veamos. Sabrían... aparentemente había una pregunta sobre si... o si no, ya saben, el RSSAC [Comité Asesor del Sistema de Servidores Raíz] y el SSAC [Comité Asesor de Seguridad y Estabilidad] están invitados a esta reunión. Bueno, (a) es una reunión abierta, (b) puede haber habido alguna confusión porque nosotros... ¿qué reunión fue esa? ¿la de Marrakech? Olvidé que reunión, pero tuvimos que rebotar... tuvimos que cancelar el TEG para hacer cosas relacionadas con la transición; de modo que, en lugar de tener la reunión del TEG, decidimos

realizar un cóctel del TEG y la Junta Directiva, y simplemente para hacer las cosas un poco más entretenidas, también participamos al RSSAC y al SSAC. De modo que fue el cóctel de la Junta Directiva, el TEG, el SSAC y el RSSAC, que se ha convertido en una especie de semitradición, es decir, los miembros del TEG y los miembros de la Junta Directiva son bienvenidos a participar en el TE.... el cóctel esta noche en la sala Ruby a eso de las 7:00 o algo así.

>> 7:00.

DAVID CONRAD: 7:00, con un autobús que sale a las 6:45 del frente de...

En realidad, tienes un micrófono.

>> Así que, después de la sesión, a las 6:45 tenemos un servicio de traslado, que es un vehículo bastante grande, en la entrada oeste del Bella Center, justo a la vuelta de la esquina desde aquí.

A las 6:45, por favor vengan a bordo y únase a nosotros. Gracias.

DAVID CONRAD: Y Steve ha llegado, de modo que al igual que con Jonne, la fiesta puede comenzar.

>> (Fuera del micrófono.)

DAVID CONRAD: Exactamente. ¿Quisiera decir algo?

STEVE CROCKER: Seguro. Me disculpo por haber llegado tarde. Estoy completamente encantado de ver tanta gente aquí. Esto es fantástico. David está a cargo.

[Risas]

DAVID CONRAD: Bien. De modo que, comencemos con las presentaciones.

Marc, ¿quisiera? Su nombre, sí, empresa, color favorito. No lo sé.

MARC BLANCHET: Marc Blanchet.

JAY DALEY: Soy Jay Daley, de .nz

DANIEL DARDAILLER: Daniel Dardailler, W3C [Consorcio Mundial de Internet]

LITO IBARRA: Lito Ibarra, Junta Directiva de la ICANN.

KAVEH RANJBAR: Kaveh Ranjbar, ambos técnico y Junta Directiva de la ICANN.

LARS JOHAN-LIMAN: Lars Johan-Liman, director de operaciones del servidor raíz de Netnod.

GEORGE SADOWSKY: George Sadowsky, Junta Directiva de la ICANN

RINALIA ABDUL RAHIM: Rinalia Abdul Rahim, Junta Directiva de la ICANN

PATRIK FÄLTSTRÖM: Patrik Fältström, Presidente del SSAC [Comité Asesor de Seguridad y Estabilidad]

ASHWIN RANGAN: Ashwin Rangan, Personal de la ICANN.

CHERINE CHALABY: Cherine Chalaby, Junta Directiva de la ICANN.

MARKUS KUMMER: Markus Kummer, Junta Directiva de la ICANN.

TERRY MANDERSON: Terry Manderson, Personal de la ICANN, Director de Ingeniería del DNS [Sistema de Nombres de Dominio] y Director de Área en el IETF [Grupo de Trabajo en Ingeniería de Internet] para el área de Internet.

ALAIN DURAND: Alain Durand, Personal de la ICANN, investigación en OCTO.

ASHA HEMRAJANI: Asha Hemrajani, Junta Directiva de la ICANN.

PAUL VIXIE: Paul Vixie, invitado, Farsight Security.

JEREMY RAND: Jeremy Rand, proyecto Namecoin.

PAUL WOUTERS: Paul Wouters, Coordinador de Enlace del IETF.

STEVE CROCKER: Steve Crocker, Junta Directiva de la ICANN.

DAVID CONRAD: David Conrad, Organización de la ICANN.

STEVE CONTE: Steve Conte, Personal de la Organización de la ICANN.

CATHY PETERSEN: Cathy Petersen, Personal de la Organización de la ICANN.

WENDY PROFIT: Wendy Profit, Personal de la Organización de la ICANN.

JONNE SOININEN: Jonne Soininen, Coordinador de Enlace del IETF con la Junta Directiva de la ICANN.

DAN YORK: Dan York, Sociedad de Internet con enfoque en las DNSSEC [Extensiones de Seguridad del Sistema de Nombres de Dominio].

SUZANNE WOOLF: Suzanne Woolf, SSAC, RSSAC [Comité Asesor del Sistema de Servidores Raíz], alborotadora al azar.

WARREN KUMARI: Warren Kumari, Coordinador de Enlace del IETF.

ED LEWIS: Ed Lewis, Organización de la ICANN, investigación en OCTO.

ROY ARENDS: Roy Arends, ICANN, investigación en OCTO.

MATT LARSON: Matt Larson, también investigación en OCTO, ICANN.

FRANCISCO DA SILVA: Francisco da Silva de ETSI [Instituto Europeo de Normas de Telecomunicaciones] y mi compañía es una empresa multinacional de Suecia.

HOWARD BENN: Howard Benn, también representando a ETSI.

JULIE HAMMER: Julie Hammer, SSAC.

ROD RASMUSSEN: Rod Rasmussen, SSAC.

>> (mencionando nombre) del ITU-T [Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones].

ADIEL AKPLOGAN: Adiel Akplogan, Personal de la Organización de la ICANN, participación técnica.

GREG AARON: Greg Aaron, SSAC.

MAARTEN BOTTERMAN: Maarten Botterman, Junta Directiva de la ICANN.

JAAP AKKERHUIS: Jaap Akkerhuis, SSAC y Comité de Trabajo del RSSAC.

LOUSEWIES VAN DER LAAN: Disculpas por llegar tarde. Lousewies Van der Laan, Junta Directiva de la ICANN.

JOHN CRAIN: Estaba escondido al fondo y pensé que debía venir al frente. John Crain, Organización de la ICANN, Director Ejecutivo de SSR (Seguridad, Estabilidad y Flexibilidad).

DAVID CONRAD: Bien. Muchísimas gracias.

Así que, la agenda está en pantalla. Esta es una sesión administrativa y de bienvenida.

Sólo para reiterar lo que dijimos anteriormente, si está buscando la reunión del grupo de dirección de aceptación universal, se ha trasladado a la sala B5.1, que está justo al final del pasillo. Sin embargo, aquí también le damos la bienvenida. Este es, por supuesto, el juego de jaula del Grupo de Expertos Técnicos versus la Junta Directiva.

A continuación, supongo que comenzaremos con una presentación de Jeremy Rand del Proyecto Namecoin, quien nos hablará acerca de Namecoin. De modo que Jeremy, si desea comenzar.

JEREMY RAND: Hola. Soy Jeremy Rand de Namecoin, así que vamos a empezar.

Primero una completa transparencia. Soy uno de los desarrolladores más activos de Namecoin y no conozco a ningún desarrollador de Namecoin que pueda estar en desacuerdo con nada en esta conversación. Sin embargo, no puedo hablar sobre todas las cosas por todos los desarrolladores. Somos un proyecto de código abierto que no tiene una estructura organizativa clara, así que sólo sepan eso.

Esta charla fue preparada en colaboración con Hugo Landau.

De modo que la motivación subyacente de Namecoin es que los seres humanos se comportan de forma no determinística y, por extensión, cualquier sistema dirigido por seres humanos se comportará de forma no determinística.

Y en particular, incluso si un sistema tiene reglas básicas que se supone que son inviolables, las reglas de base que son impuestas por los seres humanos se aplicarán de manera incoherente.

Como, por ejemplo, la Constitución de los Estados Unidos establece reglas básicas que dicen que la tortura y la vigilancia masiva están fuera de los límites. Desafortunadamente, esas reglas básicas son impuestas por los seres humanos y, por lo

tanto, como todos sabemos, esas reglas no se aplican en ningún modo tan determinista como podríamos esperar.

Y en el futuro lejano, la conducta humana es aún más no determinista.

Por ejemplo, predecir los resultados de las elecciones se vuelve más difícil cuanto más en el futuro son y, por lo tanto, predecir el clima político en un país es, por consiguiente, más difícil a medida que más se avanza en el futuro.

Y el DNS es, en gran parte, dirigido por seres humanos. Esto plantea un riesgo porque las personas involucradas en el funcionamiento del DNS podrían comportarse de manera no determinista.

Tal vez su Registrador comete un error y deja que alguien cambie sus registros, o tal vez el gobierno que posee su ccTLD [Dominio de Alto Nivel con Código de País] podría ser derrocado en 10 años a partir de ahora y el nuevo gobierno decide que no le gusta su nombre y decide incautarlo; o tal vez la presión política da lugar a que en el futuro la ICANN implemente una nueva política con la cual ahora ustedes no estuvieron de acuerdo.

Y cualquiera de estas cosas podría ocurrir y esto es preocupante.

De modo que, Namecoin es un experimento para averiguar si es posible construir algo que sea vagamente similar al DNS, pero con la menor participación humana que sea posible, y así crear un sistema similar al DNS que se comporte de forma más determinista de lo que lo hace el DNS. Y la esperanza aquí es que esperamos que un sistema como ese sea más confiable y más seguro contra los modos de falla que son causados por los seres humanos, porque el sistema es más determinista.

Por lo tanto, veamos algunos sistemas de identificadores existentes para que podamos ver cómo se comparan con Namecoin.

Los nombres manuales de un sitio, cosas como los archivos de host, no tienen un espacio de nombres global, lo cual significa que los nombres sólo tienen sentido a nivel local, pero están a salvo de terceros humanos no deterministas y tienen nombres humanos con significado, de modo que eso es bueno.

El nombre jerárquico, como el DNS, tiene un espacio de nombres global pero no está a salvo de terceros humanos no deterministas. Tiene nombres humanos con significado. Esto plantea una buena facilidad de uso, pero es arriesgado como una raíz de confianza.

El direccionamiento de contenido como BitTorrent, donde el nombre es el hash, tiene un espacio de nombres global y está a

salvo de terceros humanos no deterministas, pero no tiene nombres humanos con significado y el contenido nunca puede cambiar.

Una variante de eso es el nombre, es la clave pública. Cosas como los dominios .ONION que utiliza Tor. Éstos tienen un espacio de nombres global y están a salvo de terceros humanos no deterministas, pero nuevamente no tienen nombres humanos con significado. Sin embargo, el contenido puede cambiar. Este tipo de sistema es seguro como una raíz de confianza, pero tiene muy mala funcionalidad de uso. El usuario verá una URL como se ve en la pantalla cuando intente escribir algo.

En realidad, estoy mintiendo. Tor está haciendo una actualización de seguridad en este momento y cuando terminen, los nombres se verán así.

[Risas]

JEREMY RAND: Sí. Puede que hayan notado en las diapositivas precedentes que había dos verificaciones y una X, y éste es Triángulo de Zooko. Por lo tanto, Zooko Wilcox conjeturó que era imposible lograr los tres de ellos a la vez.

Pasando a un tema ligeramente diferente, los registros públicos del tipo append-only [sólo agregado] están viendo una creciente popularidad para garantizar la responsabilidad en la rendición de cuentas. El ejemplo más exitoso de esto es la transparencia del certificado de Google. Cada certificado único que se utiliza en la web pública está siendo agregado a un registro append-only y, eventualmente, los navegadores probablemente requerirán que los certificados estén registrados para ser válidos. E incluso si desea mantener el control sobre un sistema, es posible que desee que se publiquen todas las acciones.

La transparencia del certificado es un registro append-only para certificados, pero no es muy adecuado para su uso con sistemas como el DNS, y la razón de ello es: ¿quién puede escribir en el registro? Cualquiera. Pero sólo se pueden escribir certificados de autoridades de certificación reconocidas. Esto es bueno para asegurar que los registros no se envíen como correos electrónicos no deseados con datos no deseados, pero una lista manual de entidades de confianza es algo engorrosa.

Namecoin es un registro append-only para la registración de nombres y actualizaciones. Sin embargo, a diferencia de la transparencia del certificado, Namecoin se implementa usando una cadena de bloques, por lo cual puede prevenir correos electrónicos no deseados al imponer un costo económico para escribir datos, y este costo es pequeño pero muy efectivo, y esto

desincentiva a los actores maliciosos respecto a la ocupación ilegal (*squatting*) masiva de nombres, sin depender de una lista manual de entidades de confianza.

Namecoin tiene un espacio de nombres global, está a salvo de terceros humanos no deterministas y tiene nombres humanos con significado, de modo que es una solución al Triángulo de Zooko. Namecoin significa que un registro append-only para nombres puede funcionar como un foro abierto, mejorando su utilidad. Por lo tanto, la responsabilidad y la transparencia pueden hacerse un bien público criptográficamente verificable. E independientemente del sistema de reglas que Namecoin utiliza para los nombres, su naturaleza como un registro append-only significa que, si un actor malicioso hace algo, siempre se sabe.

Como idea experimental, considere la idea de una zona raíz responsable. La responsabilidad puede satisfacer a partes, que de otro modo sospecharían, de que en realidad no existe nada sospechoso.

Como un ejemplo hipotético, el mantenimiento de la zona raíz como un registro append-only para satisfacer a los países en todo el mundo respecto a que el control de los EE.UU. no está siendo abusado, incluso a nivel intergubernamental.

Los servidores raíz pueden alimentarse directamente desde el registro. Una zona raíz mantenida como un registro append-only podría satisfacer a países respecto a que, por ejemplo, su ccTLD [Dominio de Alto Nivel con Código de País] no se verá interferido por razones políticas, algo análogo al monitoreo sísmico usado por los países para comprobarse entre sí bajo el tratado de prohibición de pruebas nucleares, asegurando la paz. Confiar pero verificar. Y para ser claro, no estoy recomendando que esta idea en particular sea implementada en el DNS, sino que es un estudio de caso hipotético interesante.

Cambiando ligeramente la marcha, un problema relacionado es la infraestructura de la clave pública TLS [Seguridad de la Capa de Transporte]. El sistema de autoridad del certificado que se utiliza hoy en día es problemático, incluso con la transparencia del certificado. Y el problema subyacente aquí es que hay demasiados humanos no deterministas implicados, que pueden cometer errores. Las DNSSEC [Extensiones de Seguridad del Sistema de Nombres de Dominio] y la DANE [Autenticación Basada en el DNS de Entidades Nominadas], las cuales almacenan datos TLS en el DNS en lugar de que las autoridades de certificación los verifiquen, podrían mejorar la situación. Lamentablemente, también existen problemas políticos. Algunas personas están nerviosas por la posibilidad de abuso

por parte de la raíz del DNS o los operadores de TLD [Dominios de Alto Nivel].

Y, de nuevo, el problema aquí es que la raíz del DNS y los operadores de TLD también tienen humanos involucrados. De modo que no resuelve completamente el problema de la participación de humanos. Namecoin podría proporcionar las ventajas de las DNSSEC y la DANE para este propósito, sin los problemas políticos.

Por lo tanto, no esperamos que la mayoría del software o incluso la mayoría de las bibliotecas de resolución de nombres estén al tanto de Namecoin directamente. En su lugar, esperamos que el software de puente Namecoin-a-DNS se instale localmente, traduciendo consultas al DNS en consultas a Namecoin y convirtiendo nuevamente las respuestas desde Namecoin al DNS.

Namecoin utiliza el dominio de alto nivel .BIT, y en la actualidad esto no está registrado con la ICANN o el IETF. Y nos gustaría encontrar una manera viable de arreglar eso. Nos damos cuenta de que es un problema. Por ejemplo, podríamos usar los Registros de nombres de uso especial, tal como .ONION fue utilizada por Tor.

Nuestra referencia de limitación llamada NCDNS actúa como un servidor del DNS autoritativo para el dominio de alto nivel .BIT,

que se ejecuta en un host local. Los usuarios de las DNSSEC generan un tiempo de instalación e intencionalmente tratamos de mantener la especificación de nombre de dominio de Namecoin fácilmente asignable al DNS, para que el software de puente se pueda utilizar con facilidad.

Si, hipotéticamente, usted quisiera usar esto, podría indicar a su servidor del DNS recursivo, por ejemplo: que Unbound utilice al NCDNS como autoritativo para .BIT y le suministre la clave pública de las DNSSEC de NCDNS. En teoría, todo debería funcionar. Y estas son sólo unas pocas líneas de unbound.com.

En la práctica, hay algunas características del DNS que no son muy ampliamente compatibles. Por ejemplo, la DANE para la TLS. Por lo tanto, tenemos que hacer algunas extrañas adaptaciones de multiplicación para hacer que las cosas funcionen. Y en realidad estaba intentando hacer un seguimiento de cuántas capas diferentes de locos hechizos estábamos usando para hacer que la DANE de Namecoin funcione correctamente para los navegadores que no soportan la DANE para la TLS. Y dejé de contar en cinco capas de hechizos.

Entonces, ¿cuáles son algunos casos de uso del mundo real donde el comportamiento determinístico de Namecoin puede ayudarnos? Bueno, digamos que usted está tratando de

comprar o vender un nombre. En el DNS, la compra o venta de un nombre suele implicar algún riesgo de la contraparte, y es posible que tenga que confiar en un agente de custodia de datos para mitigar ese riesgo de la contraparte.

En Namecoin, el comprador y el vendedor pueden construir conjuntamente una transacción que pague al vendedor y transfiera el nombre al comprador en forma atómica. Y esto elimina el riesgo de la contraparte sin requerir a los servicios de un agente de custodia.

Y eso es estupendo, pero ¿qué ocurre si el comprador y el vendedor ni siquiera quieren hablar entre sí a fin de establecer la transacción atómica? Usted puede comprar o vender ofertas. Y el flujo de trabajo funciona como algo así. Alice puede crear una oferta de venta. Estoy dispuesto a vender el nombre de dominio ejemplo.bit por 100 Namecoins. Y Alice firma la oferta de venta con su clave privada que demuestra que es propietaria de ejemplo.bit y está dispuesta a transferirlo a cambio de 100 Namecoins. Y Alice puede publicar esta oferta de venta firmada en un foro o pastebin o cualquier cosa de ese tipo.

Bob ve la oferta y quiere comprar ejemplo.bit. Bob puede completar la oferta firmándola con una clave privada que posee 100 Namecoins. Y esta oferta es ahora una transacción válida de

Namecoin. Bob puede luego transmitir a la red Namecoin sin contactar a Alice de nuevo.

Alice recibe el pago. Bob obtiene el dominio. Y esta transacción es atómica. No hay riesgo de la contraparte, y no hay un agente de custodia necesario. Y esto funciona tanto para ofertas de compra como para ofertas de venta. El protocolo Namecoin soporta este caso de uso, y es de esperar que pronto vengan las herramientas de uso amigable.

Además, otro ejemplo de caso de uso es que un nombre suele ser propiedad de una sola clave privada, pero también se puede hacer de propiedad múltiple con varias claves privadas, donde deben estar presentes las claves M-de-N para que una actualización pueda emitirse. Y esto puede ser una protección útil contra una única clave comprometida. Por ejemplo, una Junta Directiva puede tener una clave privada y actualizar el nombre podría requerir de una mayoría calificada del directorio. Y, una vez más, el protocolo Namecoin soporta este caso de uso, y es de esperar que pronto vengan las herramientas de uso amigable.

Namecoin también puede permitir la creación de políticas de actualización muy flexibles, que se pueden utilizar para adaptar las cosas en función de las necesidades de seguridad y experiencia del usuario de un propietario de nombre en

particular. Por ejemplo, digamos que Alice posee un nombre pero desea limitar el riesgo de que su clave privada sea robada, aunque sin introducir demasiado riesgo de la contraparte. Entonces puede crear una política que es algo como esto: Alice puede contratar a Trent para que ejecute un servicio de autenticación de dos factores. Entonces Alice puede actualizar su nombre con datos arbitrarios, si Trent firma sus actualizaciones. Y Trent promete sólo hacer esto después de verificarlo, a través de la autenticación de dos factores.

Pero además, Trent puede realizar una firma previa de transacciones específicas para ciertos eventos en los que Alice quizás quiera hacer algo sin la aprobación de Trent más tarde. Por ejemplo, tal vez Alice desee poder revocar su registro TLSA de modo que, si su servidor web se encuentra en peligro, ella puede revocar el certificado fácilmente. O tal vez a Alice le preocupa que Trent pueda desaparecer o salir de negocios o perder su clave privada. Por lo tanto, estas políticas se pueden especificar sobre la base de restricciones muy adaptables. Trent no puede transferir o actualizar el nombre de Alice sin la firma de Alice, y Alice puede verificar que las transacciones preseleccionadas son auténticas y que está protegida de Trent antes de aplicar esta política a su nombre. Y estas políticas se especifican en un lenguaje de secuencias de comandos y se aplican al mismo nivel que las firmas estándar.

Namecoin no significa que los Registradores desaparecen. En Namecoin, los "registradores" podrían parecerse mucho a Trent. Sin embargo, Namecoin significa que los Registradores tienen mucha menos capacidad de dañar a sus clientes que en el DNS, ya sea en forma accidental o por daños maliciosos. Y esto podría terminar resultando en la necesidad de que los Registradores reduzcan los presupuestos de seguridad.

Aún no existen para Namecoin servicios como Trent, pero me gustaría ver un servicio como este. Como otro caso de uso, la infraestructura del DNS ha sido objeto de recientes ataques de DDOS [Denegación de Servicio Distribuido], por ejemplo, el ataque contra Brian Krebs. Y algunas personas han sugerido que Namecoin podría ser una defensa útil. Ahora, no está claro para mí exactamente cuán bien Namecoin se enfrentaría a un ataque de DDOS.

Sin embargo, en los últimos años, la red de Bitcoin ha sido sometida a pruebas de tensión, que son básicamente intentos de ataque de DDOS. Las pruebas de estrés fueron realizadas por compañías con fines de lucro que tenían un incentivo financiero para tratar de hacer que la red de Bitcoin parezca débil frente a tales ataques. Y Bitcoin no fue afectado. ¿Se comportaría Namecoin de la misma manera? ¿O los atacantes tendrían incluso recursos similares a las pruebas de estrés de Bitcoin? Es

difícil de decir. Pero creo que es un caso de uso interesante. Me gustaría ver más investigaciones sobre esto en el futuro.

Sin embargo, para tener este determinismo necesitamos realizar algunas compensaciones. Como ejemplo, las transacciones de Namecoin son irreversibles. Y como resultado, si un nombre se transfiere a un nuevo propietario, el propietario antiguo no puede recuperarlo sin la firma del nuevo propietario. Esto significa que los nombres de Namecoin son algo más vulnerables a la adquisición hostil mediante malware. Y para esa materia, el error humano por parte del dueño del nombre también podría ser un problema.

Algunos aspectos de este problema incluirían el mantenimiento de sus claves privadas en una máquina con espacio libre o, posiblemente, la asignación de políticas de autenticación con múltiples firmas o de dos factores para los nombres, como he comentado anteriormente. Esto en realidad no es todo malo. He escuchado a expertos en seguridad comentar que uno de los mejores beneficios públicos de que Bitcoin se esté volviendo popular es que la gente finalmente está tomando seriamente a la seguridad desde su lugar de punto final. A medida que Bitcoin se vuelve más maduro, creo que es probable que la seguridad del punto final mejore sustancialmente. Por lo tanto, en el futuro esto puede ser un problema menor.

Otra compensación es que Namecoin no tiene una determinación humana no determinista para que las registraciones de nombre sean válidas. Y es por eso que tiene beneficios de seguridad y es más resistente a los problemas políticos. Sin embargo, eso también significa que si alguien registra un nombre que infringe una marca comercial, no hay manera fácil de deshabilitar esa registración de nombre. Se tendrá que negociar con la persona que lo registró.

Y esto es bastante inherente a la definición de infracción en materia de marcas comerciales. La determinación de si ha ocurrido una infracción requiere de un ser humano, y Namecoin está explícitamente diseñado para no ser dirigido por seres humanos.

Una forma de abordar esto sería que los usuarios puedan optar por una lista de nombres conocidos que infrinjan marcas comerciales, los cuales quedan bloqueados en algún lugar entre el cliente de Namecoin y el navegador web del usuario. Por ejemplo, el software del DNS que se utiliza como puente para las aplicaciones Namecoin-al-DNS puede admitir esto como una opción. Ya hay infraestructura para cosas como esta. PhishTank es un ejemplo.

Una advertencia es un usuario que desee ver un nombre que infrinja una marca comercial, quien intencionalmente podría

desactivar el bloqueo. Pero como el propósito de la ley de marcas comerciales es evitar la confusión del consumidor, este probablemente no sea un problema muy grande. Un usuario que hace esto probablemente ya sabe lo que está haciendo. Otra advertencia es que alguien podría comprar un nombre infractor con el único fin de venderlo al propietario de la marca comercial legítima. Pero dado que la registración de nombres cuesta dinero, es difícil para una sola persona ocupar ilegalmente una gran cantidad de nombres de esta manera, en forma similar a cómo los nombres del DNS que cuestan dinero reducen la ocupación ilegal.

Otra compensación es la privacidad. Dado que el conjunto completo de las transacciones de Namecoin es público, cualquiera puede ver las transacciones. El análisis del gráfico de transacciones hace bastante fácil averiguar si dos transacciones fueron realizadas por la misma persona. Y esto también afecta a Bitcoin. Por lo tanto, lo que esto significa es que, si usted registra dos nombres Namecoin para diferentes propósitos, probablemente sea un registro público que ambos nombres han sido registrados por la misma persona.

Y si usted compró sus Namecoins de otra persona, ellos probablemente puedan ver qué nombres registró con ellos. Una solución es comprar Namecoins con un método de pago que no deje un registro público. Lo que significa que, si valora su

privacidad, no debe usar Bitcoins para comprar Namecoins. Y también debe usar pares de claves públicas y privadas por cada nombre que compre, para que no se puedan enlazar en el gráfico de transacciones. Las transferencias bancarias pueden ser una buena manera de comprar Namecoins sin dejar un registro público. Y además, hubo esfuerzos experimentales para hacer que divisas del tipo Bitcoin tengan una mayor privacidad, tal como Monero y Zcash que se podrían utilizar para comprar Namecoins y entonces obtener los nombres. Tienen sus propios inconvenientes, pero pueden valer la pena para algunos usuarios.

Y, en general, la implementación de referencia de Namecoin tiene una privacidad muy pobre y hace difícil impedir que el público conozca que todos sus nombres tienen una propiedad común. Queremos hacer mejoras sobre esto, porque este es un asunto importante.

La última compensación es la seguridad de la naturaleza append-only de Namecoin. Todas las propiedades de seguridad que Namecoin tiene son criptográficamente verificables, con una excepción importante, y es que la protección del orden de las operaciones de nombre Namecoin no es criptográficamente segura. En su lugar, sólo es económicamente segura, lo que significa que costaría mucho dinero reordenar las operaciones de nombre. Y cuanto más atrás en el tiempo se vaya, más dinero

costaría. Normalmente Namecoin supone que el orden es probablemente inmutable hasta alrededor de las dos horas posteriores a que una operación de nombre toma lugar. Pero esto no está garantizado criptográficamente. Esto es de naturaleza probabilística y económica, por lo cual es mucho más débil.

Entonces, ¿cómo podría usarse esto para un ataque práctico? Bueno, si usted pudiese cambiar el orden de las operaciones que se remontan a cuando se registró un nombre, se podría colocar una operación de registración para ese nombre antes de la registración legítima y, por lo tanto, robar el nombre.

También se podría cambiar el orden de las operaciones de renovación del nombre que ocurran en forma posterior al período de vencimiento, lo cual obliga el vencimiento del nombre y habilita su registración. Nada de esto ha ocurrido en la vida real de Namecoin. Pero si Namecoin gana una adopción creciente, más personas podrían intentar hacerlo.

Bitcoin tiene el mismo problema aquí. Pero dado que la economía de Bitcoin es mucho más grande que Namecoin, Bitcoin gana mucha más seguridad contra los ataques. Y existe una gran investigación activa para resolver este problema de cadenas de bloqueo secundarias que son menos seguras que Bitcoin. Y eso es en parte porque muchas mejoras a Bitcoin,

incluyendo algunas que están siendo impulsadas por compañías muy bien financiadas, son mucho más fáciles de implementar si se resuelve este problema. De modo que estamos atentos y observando esta área de investigación muy de cerca. Y esperamos progreso pronto.

Ninguna de las formas de solución que acabo de describir para el malware, las marcas registradas y la privacidad son absolutamente tan directas como las contramedidas tomadas con el DNS. Y encontrar soluciones más elegantes es un problema de investigación abierto. Dicho esto, para muchos casos de uso del mundo real, probablemente estas soluciones sean suficientes.

Bien. Entonces, ¿dónde va el desarrollo? Bueno, desafortunadamente, ahora mismo Namecoin es realmente difícil de instalar, especialmente si se desea que el soporte de TLS funcione. Y eso es principalmente porque no es muy automatizado en el proceso de instalación. Acabamos de recibir fondos de la Fundación NLNet y el Fondo para la Solidificación de Internet, con presupuesto del Ministerio de Asuntos Económicos de los Países Bajos. Esta financiación se usará para mejorar la funcionalidad de uso y el soporte de aplicaciones para el uso de Namecoin como una infraestructura de clave pública de TLS. Y el objetivo final aquí es que la integración de Namecoin con el sistema de resolución de nombres de una

computadora y con las implementaciones de TLS de los principales navegadores web pueda instalarse en un solo paso. De modo que, por ejemplo, si usted está en Windows, ejecute un instalador .exe. Si usted está en Debian, ejecute un paquete .deb.

Y esta financiación también se usará para mejoras a la experiencia del usuario para los propietarios de nombres, y para mejoras sobre la capacidad de ampliación y el desempeño. Y este trabajo está siendo principalmente realizado por mí, Hugo Landau, Brandon Roberts y Joseph Bisch.

También estamos participando activamente con el proyecto Tor. La base de usuarios de Tor tiene requisitos de seguridad específicos que no son muy adecuados para el DNS. Ahora ellos están usando .ONION, que no tiene significado humano, y esto va a empeorar cuando su actualización a la versión 3 de los Servicios de Onion se ponga en marcha, tal como he mostrado antes. Y el problema es que psicológicamente los humanos no suelen comprobar el despliegue de la dirección onion, lo cual significa que ahora los delincuentes existentes están creando imágenes previas parciales de las direcciones .ONION existentes para imitarlas/suplantarlas. Y Tor es un buen candidato para la adopción temprana de Namecoin. Ellos probablemente pueden vivir con el estado actual de las compensaciones de Namecoin, con la posible excepción de los problemas de privacidad, porque

todas las otras opciones disponibles simplemente no cumplen con los requisitos de seguridad de Tor. Y yo soy quien actualmente está liderando el alcance del proyecto Tor.

Y la última área de desarrollo está en el back-end, tenemos un hardfork [cambio radical al protocolo] próximamente, el cual —si no está familiarizado con la terminología de la cadena de bloques— constituye una actualización que rompe la compatibilidad hacia atrás por completo. Y esto fue necesario porque Bitcoin puso en marcha algunas mejoras a su sistema que no podemos adoptar sin romper la compatibilidad hacia atrás, y queremos estar cerca de Bitcoin.

También estamos viendo varias otras mejoras, cosas como hacer que el período de vencimiento sea mucho más fácil de usar, tener pruebas de contacto de no existencia para poder corroborar fácilmente si un nombre no existe, permitir que los nodos de punto de nombre descarten datos antiguos para mejorar la capacidad de ampliación. Los hashes aún se conservarían para que los datos descartados aún puedan comprobarse, y también permitir que los Namecoins se compren usando Bitcoins, o tal vez Monero o Zcash, sin ningún riesgo de la contraparte. Y la mayoría de estos esfuerzos están siendo dirigidos por Daniel Kraft.

Así que, gracias por invitarme. Tomaré cualquier pregunta gustosamente.

DAVID CONRAD: Bien. Gracias Jeremy. Tenemos unos minutos para preguntas y respuestas, si alguien tiene alguna pregunta. Sí Steve.

STEVE CROCKER: Sin duda, esta es una gran presentación. Muchísimas gracias.

JEREMY RAND: Gracias.

STEVE CROCKER: Yo estaba prestando atención respecto al nivel de protección y qué tipo de cosas pueden salir mal. La protección fuerte es que todos los cambios que se hacen son conocidos, como yo lo entiendo. El... y por lo tanto, en el escenario para, digamos, un cambio de la zona raíz, si adoptásemos esto, si... si alguien cambiase algo en la zona raíz, se sabría. Eso es un nivel de protección, pero un problema diferente en el cual algunas partes están interesadas es cómo puedo evitar una acción adversa en contra de mi dominio de alto nivel para que simplemente no sea posible. Y tal vez las semillas de eso se encuentran en que M de N combinados con la posibilidad de que la persona normal... la persona que normalmente haría el

cambio, su clave funcionará y se utilizarían otras claves en concierto para una anulación o algo como eso. Pero no estaba 100% claro para mí que eso es todo lo que puede suceder.

JEREMY RAND: Sí. De modo que sí, definitivamente puede utilizar Namecoin con el fin de evitar que los ataques maliciosos en realidad sucedan. Cosas como el método de firma múltiples, que son las firmas M de N, definitivamente pueden ser beneficiosas para eso. Y al igual que el ejemplo que daba con la política de autenticación de dos factores, que también se puede utilizar para eso.

Así que, sí, creo que hay varios casos de uso aquí. Un caso de uso es asegurarse de que cualquier cosa maliciosa que suceda es conocida públicamente y no se puede borrar de la memoria. Pero sí, tiene toda la razón, en cuanto a que es importante poder intentar hacer que los ataques sean tan difíciles de lograr en primer lugar como sea posible. Y sí, Namecoin puede ayudar con eso. Dado que... dado que el sistema Namecoin fue diseñado originalmente para... para los usuarios finales que poseen un nombre de dominio estándar, una idea sería: bien, si le preocupa que su Registrador pueda dañar su nombre de alguna manera, ellos podrían permitir que alguien lo actualice por accidente, si lo desea, con Namecoin usted puede ser su

propio registrador. De modo que no es necesario confiar en un tercero, a menos que desee... a menos que desee que ellos confíen en una protección adicional, como la firma múltiple.

STEVE CROCKER: Hay una serie de casos en los cuales es posible que se necesite la intervención de terceros, la asignación del nombre en primer lugar, la recuperación de las claves si se han perdido, la prevención o la reacción al comportamiento deshonroso, etcétera. Por lo tanto, tengo problemas para prever una variación en el sistema que tenemos que no tiene vías para ese tipo de transacciones, y, por supuesto, tan pronto como lo hagan, entonces tienen que exponer que se puede obtener un comportamiento deshonroso por parte del operador excepcional, y por lo tanto es... una cuestión de encontrar un buen ajuste entre ellos.

JEREMY RAND: Correcto. Sí. De modo que...

STEVE CROCKER: Oh, y una cosa más.

JEREMY RAND: Seguro.

STEVE CROCKER: El tipo de operadores deshonestos que nos preocupan no estarían preocupados en absoluto por ser descubiertos.

JEREMY RAND: Sí, definitivamente podría creer eso, sí. Sí, así que... sí, definitivamente existe una compensación entre la capacidad de un ser humano para corregir el comportamiento malicioso que sucedió versus la capacidad de un... de un usuario legítimo de estar convencido de que un ser humano no será capaz de causar daño a su propio nombre. Y sí, esta es una compensación fundamental. No hay un muy... no hay una buena manera de obtener ambos tipos de protección a la vez. Por esta razón, es posiblemente poco probable que Namecoin reemplace completamente al DNS en el corto plazo. De hecho, me imagino que hay un gran número de usuarios que prefieren al DNS sobre Namecoin, por esta razón. Dicho esto, creo que también hay una importante base de usuarios que quiere... las compensaciones que Namecoin hace y que están dispuestos a soportar... a correr con el riesgo de que, si alguien las roba la clave privada, el juego... el juego se terminó. Pero sí, es sin duda un problema abierto de investigación en cuanto a cómo hacer que la protección de sus claves privadas sea tan buena que...

que el riesgo sea insignificante. Y sí, este es un problema abierto de investigación.

STEVE CROCKER: Seguimiento rápido. Mi lectura de la tecnología actual es que robar una clave privada es insignificante. Quiero decir, se coloca en un montón de hardware que si se sacude un poco... pero el intercambio es que tienes un riesgo mucho mayor de perder el control si tu clave privada se destruye o se pierde o algo así. Por lo tanto, esa es la acción que requeriría la recuperación.

JEREMY RAND: Sí. De modo que si no está preocupado acerca de que una parte maliciosa obtenga su clave, pero considera que usted puede asegurarse de que... pero usted está principalmente preocupado acerca de que su clave pueda simplemente ser destruida por accidente, entonces sí. Entonces puede tener una clave de seguridad disponible. Podría, por ejemplo, tener una política de firma múltiple en la cual... que es 1 de N. De modo que usted podría tener N copias de seguridad; lo siento, N menos 1 copias de seguridad. N1 significa que usted podría utilizar la clave principal para todo, y también podría aplicar un registro de tiempo para que las claves de seguridad sólo puedan utilizarse para recuperar el nombre, en caso que la clave principal sea destruida y, digamos, pasen seis meses. Lo cual no es suficiente

para que el nombre venza, pero hace que, por ejemplo, si alguien intenta usar maliciosamente una de las claves de seguridad, no pueden usarla a menos que ya haya perdido la clave principal también. Así que, sí, es un sistema bastante flexible. Pero sí, en algún momento usted está confiando en que una cierta cantidad de claves no se perderán.

DAVID CONRAD: Bien. Tenemos un par de minutos más para preguntas. Asha.

ASHA HEMRAJANI: Sí, gracias David. Gracias por esta presentación. Tengo que decir que no entendí casi como las tres cuartas partes de esto, así que esto es lo que lo simplifiqué en mi cabeza y quería ver si es correcto. De modo que, una forma de prevenir los ataques y... entonces en lugar de... entonces en lugar de que su nombre de dominio esté bajo riesgo de, digamos, un gobierno o un Registrador, el DNS funciona en su propia computadora, la guía telefónica digital está de algún modo en su propia computadora.

JEREMY RAND: Sí.

ASHA HEMRAJANI: Y entonces Bitcoin de algún modo asegura que cada computadora en el mundo tiene esa misma guía telefónica digital o mismo DNS, ¿sería esa una descripción correcta?

JEREMY RAND: Sí. Sí, ese es un resumen excelente. Sí.

ASHA HEMRAJANI: Bien, muy bien. Uf. Bien. Entonces deseo volver a lo de .BIT que mencionó antes en sus diapositivas. De modo que, esto ahora se está refiriendo a los sitios web de .BIT, ¿no es cierto?

JEREMY RAND: Sí. Sí. Entonces, actualmente Namecoin está utilizando el dominio de alto nivel .BIT y, como resultado, por lo que si tiene el software Namecoin instalado interceptará cualquier solicitud del DNS para cualquier cosa que termina en .BIT y lo hará... y los verá utilizando Namecoin en lugar del DNS.

ASHA HEMRAJANI: Bien. Así que, tengo dos preguntas. Usted mencionó que .BIT no está registrado con la ICANN. ¿Es eso un requisito? Para que esto funcione.

JEREMY RAND: No es un requisito para que funcione en un nivel técnico. Quiero decir, funciona ahora, aunque no esté registrado en la ICANN. La preocupación es si, hipotéticamente, en el futuro la ICANN adjudicara el dominio de alto nivel .BIT a otra persona, entonces no estaría claro cómo se supone que el sistema funcione. Las personas que tienen el software Namecoin instalado, como está escrito ahora, estarían accediendo a los sitios web de Namecoin usando eso... usando esa búsqueda, pero las personas que no lo tienen, estarían accediendo a quien la ICANN delegue .BIT. Y las personas que intenten acceder al otro no podrían hacerlo. Y entonces existe un riesgo de colisión del espacio de nombres, básicamente. Y es por eso que nos gustaría intentar conseguir que se registre oficialmente para que no haya ningún riesgo de que, ya saben, alguien pueda intentar comprar .BIT a la ICANN en el futuro y causar problemas.

ASHA HEMRAJANI: Bien. Eso en realidad ayuda. Muchísimas gracias.

JEREMY RAND: Gracias.

DAVID CONRAD: Bien. Kaveh.

KAVEH RANJBAR: Muchas gracias por su presentación Jeremy. Tengo una pregunta rápida, porque a mi leal entender no han llevado esto al IETF aparte de un poco de discusión sobre .BIT para el Registro de uso especial. ¿Fue una elección consciente o... están planeando llevarlo a IETF o no?

JEREMY RAND: Es una buena pregunta. Así que, cuando Namecoin fue fundada, esto fue en 2011... y por cierto, eso fue antes de que yo estuviera involucrado en Namecoin, los autores originales no tenían idea de que el Registro de nombres de uso especial era una cosa. Y básicamente pensaron: está bien, sólo esperamos que la ICANN no... no delegue .BIT a nadie más; y, por supuesto, esta no fue una decisión muy sabia, pero ellos no sabían... ellos desconocían que había otra opción.

Más recientemente, cuando tres proyectos, Tor, I2P y Ganu.NET, intentaron registrar sus dominios de alto nivel a través del Registro de nombres de uso especial, nos enteramos de ello y dijimos: oh, eso suena como adecuado para nosotros también, y contactamos a los autores de ese proyecto de Internet, y nos agregaron a ese borrador de Internet. Y lamentablemente, debido a razones políticas sobre las cuales honestamente no soy la mejor persona para hablar, el borrador de Internet fue

suspendido indefinidamente. Un nuevo borrador de Internet pasó y se convirtió en una RFC [Solicitud de Comentarios] que sólo agregó a .ONION, que es Tor. De modo que los otros tres proyectos, GanuNET, I2P y Namecoin, esperan que se realicen progresos sobre esto. Pero sí, nosotros... nos involucramos activamente, y tal vez no fuimos tan rigurosos en participar como deberíamos haberlo sido. Pero sí, una vez que descubrimos que había un proceso que debíamos seguir, tratamos de seguir ese proceso lo mejor que pudimos.

KAVEH RANJBAR: Muchísimas gracias.

JEREMY RAND: Gracias.

DAVID CONRAD: Warren y Daniel... en realidad Warren y luego usted y cerramos la lista de espera para tomar la palabra porque... para la próxima presentación. Warren.

WARREN KUMARI: Por lo tanto, una de las cosas que me preocupa es que toda la propiedad del dominio está atada en la clave pública... lo siento, la clave privada, y hay muchas cosas atractivas que se pueden

hacer como M de N, etcétera, pero a los usuarios les resulta bastante difícil entender mucho de esto.

JEREMY RAND: Sí, tiene razón.

WARREN KUMARI: Digamos que como con Bitcoin puedo tener mi propia cartera privada y puedo hacer un seguimiento de todas mis cosas; sin embargo, eso es demasiado complejo para la mayoría de la gente y entonces utilizan las carteras públicas en línea que luego obtendrán propiedad. ¿Hay algún trabajo orientado a intentar hacer que sea mucho más simple, para que los usuarios sean capaces de entender qué es exactamente lo que están haciendo con esto y para mantener las cosas locales?

JEREMY RAND: Sí, hay trabajo en curso sobre eso. La mayor parte de ese trabajo está siendo realizado por la gente de Bitcoin en lugar de nosotros, sólo porque tienen muchos más recursos que nosotros. Pueden encontrar el producto GreenAddress en el mundo Bitcoin muy... bastante interesante. Básicamente, parece que es una cartera de Bitcoin que se puede instalar como una aplicación para móviles o como una extensión del navegador, cosas así. Pero tiene una autenticación de dos

factores bajo la manga. Y a menos que realmente necesite recuperar sus claves, ya saben, en el caso de que... que el servicio de autenticación de dos factores se caiga, realmente no tiene que preocuparse por la administración de las claves, cosas así. Se trata de hacer que sea tan fácil de usar como... como puede serlo. Y sí, así que realmente nos gustaría ver sistemas como GreenAddress ser utilizados con Namecoin también.

DAVID CONRAD: Bien. Y Daniel.

DANIEL DARDAILLER: Un par de preguntas. Primero, usted comenzó diciendo que el enfoque no determinista del sistema del DNS actual era un problema, pero en qué medida es un problema, ya saben, una vez que ha registrado su nombre, que pasa por el Registrador y el Registro, entonces debe ser determinista. Es la resolución de nombres, el caché, ya saben, y funciona como una transacción de un protocolo de base de datos. Entonces, ¿qué parte de lo determinista, ya saben, es el problema que están intentando resolver? ¿Es la registración en sí misma o la resolución? Esa es mi primera pregunta.

Y luego, en relación a eso, está la cuestión del desempeño. Quiero decir, hoy en día el sistema está construido para tener,

ya saben, muy buen desempeño porque hay millones de resoluciones por segundo, y el sistema que utiliza una cadena de bloques o un registro de agregado interno, la contabilidad de IP, que son... normalmente tienen que llevar al espacio de nombres de dominio completo a probar algo utilizando las claves criptográficas, así que ¿cómo funciona? Quiero decir, teniendo en cuenta las restricciones en el desempeño y la restricción del registro append-only.

JEREMY RAND: Sí. Buenas preguntas. Con respecto al no determinismo que es un problema, el ejemplo que doy estos días es que cuando originalmente se registró la URL bit.ly acotada, las personas que lo registraron probablemente no se imaginaron la idea de que: oh, el dominio .LY podría ser controlado por el Estado islámico en el futuro. Bueno, ahora hay un riesgo muy real de que ISIS acabe controlando eso y, ¿saben? ¿qué pasa si...si se aprovechan de eso?

Además, los Registradores de nombres de dominio a veces cometen errores. Esto es mucho más raro de lo que solía ser, pero en los primeros días del DNS, los Registradores de dominios han sido engañados para transferir nombres de dominio a otras personas sin la autorización adecuada, por ejemplo, enviando faxes falsificados, cosas por el estilo.

Por lo tanto, no creo que sea un riesgo muy fuerte para el caso promedio necesariamente, pero existe suficiente riesgo de que las cosas puedan salir mal como para creer que vale la pena examinar las cosas que se comportan de manera más determinista.

En lo que respecta a la capacidad de ampliación, tiene toda la razón en que las cadenas de bloqueos y las estructuras de datos append-only en general se amplían en forma más pobre que cosas como el DNS, por lo cual, sí, tiene toda la razón. Sinceramente no está claro en este punto exactamente a qué nivel puede escalar algo como Namecoin. Hubo una conversación bastante interesante sobre esto ayer en las preguntas y respuestas, cuando estaba en un panel aquí. Pero, sí, puede ampliarse un poco más de lo que es ahora. Creo que podría manejar la mayoría de los usuarios de los servicios de .ONION de Tor sin mucho problema en absoluto, lo cual sería muy beneficioso. ¿Podría reemplazar por completo el DNS hoy? Definitivamente no. ¿Podría reemplazar por completo al DNS en un futuro lejano? Es difícil de decir. Podría, pero puede que no.

DAVID CONRAD: Bien. Gracias. Supongo que tenemos un par de minutos de retraso, por lo que el siguiente orador es Paul Vixie, de Farsight Security, para hablar sobre las zonas de política de respuesta.

Paul, adelante.

PAUL VIXIE: Gracias David. Así que, mientras estemos en el tema de añadir capas de hechizos al DNS o al sistema de nombres en general porque no funciona de la manera que queremos, tengo mi propio contendiente.

Lo que quiero señalar, sin embargo, es que la ICANN ha quedado registrada, varios directores ejecutivos han sido registrados en varias ocasiones, diciendo: "No somos la policía de Internet", y esto es casi invariablemente en respuesta a alguien que desea que una baja fuese más fácil, porque habrá algún nombre de dominio en algún lugar que apunta a algunos recursos en algún lugar que está causando algún tipo de perjuicio a alguien y, ya saben, la suposición en la era previa a Internet era que todo era propiedad de alguien y si estaba siendo utilizado para hacerle daño, usted podría ir a... usted podría averiguar quién era y, o bien conseguir que le arrestaran, hacerles un juicio o al menos conseguir que reciban su reclamo y que actúen en consecuencia.

Por lo tanto, esta cosa donde Internet es... no lo sé... un servicio de blanqueo de responsabilidad donde usted sigue pidiendo que las cosas se den de baja porque le están perjudicando y resulta que no hay nadie que posee eso y todo el mundo dice:

"Lo siento, no sé quién podría conseguir bajarlo, pero no soy yo"; es muy frustrante para las personas que se ven perjudicadas por las cosas que están sucediendo en Internet.

Así que, ya saben, pueden quejarse por el clima todo lo que quieran o pueden salir y hacer algo por ustedes mismos.

Siguiente diapositiva.

Así que, todos a quienes veo a mi derecha ya saben todo esto, y todos a quienes veo a mi izquierda necesitan que se los refresque, así que para el beneficio de George Sadowsky, permítanme pasar por esto.

[Risas]

PAUL VIXIE: Hay tres capas en el flujo de datos del sistema de nombres de dominio.

En la parte inferior, tienen sus resolutores stub. Esos son todos sus smartphones, sus computadoras portátiles, cada VM, cada M. Bastante como cualquier cosa que haga una consulta al DNS es un resolutor stub. Y quiere hablar con un servidor recursivo, que francamente no es un nombre muy bueno. Necesitábamos un departamento de marketing mejor para esto.

Pero olvidando de qué tipo de recursión estamos hablando, sólo trátenlo como una palabra en blanco. Esta cosa es capaz de darle la respuesta a sus preguntas, incluyendo la respuesta negativa si hay.. si no hay respuesta, el nombre está equivocado o no hay datos, o lo que sea.

Hace esto con una memoria caché a la izquierda allí, así que eso es algo de almacenamiento. Por lo general, no es el almacenamiento en disco como se muestra en el icono de aquí pero, sin embargo, recuerda las respuestas recientes de modo que si un montón de gente pide lo mismo, no se tenga que ir a buscar por toda Internet buscando una y otra vez.

Ahora, si alguien le pregunta algo que no está en su caché, entonces usted tiene que hacer eso. Tiene que subir al nivel superior, que es donde la ICANN realmente vive. El mundo de la ICANN son los servidores de autoridad. Los servidores de nombres raíz, los servidores de TLD, los servidores de TLD efectivos, los Registros, los Registradores, los registratarios, es todo el espacio de autoridad.

Por lo tanto, los servidores de autoridad, desde el punto de vista del protocolo, son el lugar donde el contenido entra en el sistema de nombres de dominio desde el exterior. De modo que una vez que está en el sistema de nombres de dominio, puede buscarlo utilizando el protocolo del DNS, pero antes de que se

pueda obtener, tiene que ser importado de alguna manera. Normalmente, desde un archivo de texto o una base de datos o un software. Y ese es el trabajo de las autoridades, es importar contenido al DNS desde afuera.

Por lo tanto, lo que es inusual en esta presentación en una reunión de la ICANN es que no vamos a hablar sobre los servidores de autoridad o la política por la cual se decide qué nombre crear o quién debe operar lo que sea. Ya saben, eso es lo normal, cuando yo solía venir a estas cosas mucho más a menudo, pasábamos mucho tiempo hablando acerca de los problemas del servidor de autoridad y las políticas de su entorno, y ahí es donde todo el dinero está pero, inusualmente, vamos a hablar de la capa media.

Y la razón es que las personas que están siendo perjudicadas mediante el uso de Internet como el vector de ese daño o perjuicio, realmente desean ser capaces de hacer algo, y resulta que no se puede detener a las personas que quieren dañarle a partir de la registración de nombres de dominio y la colocación de contenidos... asociando contenidos con aquellos nombres de dominio que le harán daño. Esa sería una solución de lejos. Si usted se imagina que está en un borde de Internet y que ellos están en el otro borde, sería agradable contar con una solución de lejos para evitar, no sé, la infracción de una marca comercial sería un ejemplo o la propiedad intelectual sería un ejemplo, los

materiales de abuso infantil en línea sería un ejemplo. Hay todo tipo de cosas que usted encontraría perjudiciales que quisiera no permitir entrar a Internet en el extremo lejano, pero no puede, porque, de nuevo, Internet funciona como un servicio de blanqueo de responsabilidad. Y así, a lo que hemos evolucionado, no por elección, sino por necesidad, es a una solución de cerca; algo que, dado que no puedo detenerlo lejos donde es creado, y dado que no puedo conseguir que se le dé de baja de forma fiable, voy a organizar mi punto de vista del sistema de nombres de dominio de Internet para que sea compatible con la inexistencia de lo que sea que me está perjudicando o dañando.

Y esto ha sido muy exitoso. Comenzamos este proyecto en 2011. Hemos examinado el protocolo tres veces, así que ahora estamos en el Protocolo 4. Y actualmente estamos buscando la normalización del protocolo actual, después de lo cual entregaremos el... de algún modo el control de cambios entorno al protocolo al IETF, pero en este momento el IETF ha tenido muy poco que ver con esto.

Esto realmente fue una especie de esfuerzo de equipo privado, no diferente del proyecto de código abierto como el sistema Namecoin, por lo cual algunos de ustedes han contribuido con ideas y características para esto, pero no lo han hecho a través

del IETF, sino porque pensábamos que eran inteligentes y cuidadosos de lo que decían.

Por lo tanto, lo que estamos haciendo aquí es permitir que la observación y el análisis desde el exterior se utilicen para elaborar políticas, y que esa política luego rija la respuesta, y llegaré a la "Z" en un momento, pero permítanme decir que el caché no se ve afectado por esto.

Se podría imaginar una política que dijera: "Vaya, hay una nueva botnet con algoritmos para la generación de dominios por ahí y está creando todos estos nombres. Es como Conficker o lo que sea. Y queremos asegurarnos de que, si alguien busca uno de esos nombres, no reciban una respuesta porque la respuesta podría... podría decirle a uno de mis robots o a algún cliente infectado de mi red cómo llegar a un servidor de comando y control en la red de alguien más y yo no... tengo que interceptar eso en alguna parte. Elijo interceptarlo en el DNS. "

Entonces podría decir: "Está bien, así que estos nombres, estos nombres computables que la botnet va a usar hoy en día están prohibidos", y esa podría ser la política que se establece.

Pero mañana ya no será verdad, ¿correcto? Mañana tiene un conjunto de nombres diferente. Estas botnets con algoritmos para la generación de dominios están utilizando la fecha como parte de cómo calculan qué nombre utilizar. Por lo tanto, no se

quiere bloquear el nombre todo el tiempo. Eso realmente... eso aumentaría drásticamente la probabilidad de colisión, y hay colisiones a pesar de que estos nombres...

Una botnet con algoritmo para la generación de dominios como Conficker genera nombres realmente feos, pero sí entran en conflicto con lo que pienso como nombres reales no maliciosos. Por lo tanto, desea eliminarlos.

Y entonces, no ponemos la política en el caché. En realidad ponemos la verdad en la caché.

Por lo tanto, el mecanismo de políticas de respuesta sólo afecta lo que verá un resolutor stub. No afecta lo que se almacena o lo que se obtiene de las autoridades.

Así que, les mencioné que hablaría de la "Z". La "Z" es la zona y refleja el hecho de que estos servidores recursivos ya están presentes en Internet. Hay 25 millones de ellos, la mayoría de los cuales no deberían estar allí. Son pequeños módems de cable estúpido que no deberían estar ejecutando ese servicio, pero sí. Y alrededor de 2 millones de ellos son intencionales. Y por eso hay alrededor de 2 millones de servidores recursivos que importan. Y luego está el DNS abierto y Google con su cosa de 8.8.8.8. Hay muchos servidores recursivos que importan. Y ellos son... veré cómo... ¿cómo quiero decir eso?

Queremos ser capaces de controlar la política de estos servidores utilizando datos externos, y muchos de estos servidores están bien adentro de redes existentes, protegidas como locas por firewalls para que no se pueda llegar al exterior o ser alcanzada desde el exterior.

Se considera una buena higiene de seguridad para el firewall de sus servidores de nombres recursivos, para que no sean utilizados como amplificadores de DDOS por parte de personas fuera de la red.

Pero nos dimos cuenta de que a muchos de ellos se les permite hablar al protocolo del DNS fuera de la red, por lo que decidimos que si pudiésemos escabullir la política en forma de un... de datos del DNS para ser obtenidos sobre el puerto TCP 53 de la forma en que se obtienen otros datos del DNS, que probablemente funcionaría, y estos servidores recursivos podrían suscribirse a una fuente de política. Por lo tanto, comenzó el experimento de intentar insertar la política de respuesta en la forma de una zona del DNS.

De modo que esto sería... esta es la zona del DNS más fea que pueda ver. Está llena de patrones que están destinados a no ocurrir en la naturaleza, y entonces es realmente antinatural y es realmente horrible de ver.

Es algo de lo que uno podría estar orgulloso de lo horrible que es, como si lo horrible fuese un proyecto de arte en sí mismo.

Por lo tanto, el flujo de trabajo aquí es que alguien en la parte superior derecha hace la observación y el análisis. Ellos piensan: "Bueno, una nueva botnet, un nuevo DGA [algoritmo para la generación de dominios], un nuevo conjunto de nombres que no deberían resolverse hoy", o quizá sea un nuevo bloque de direcciones IP que es conocido por estar siendo utilizado por un remitente de correo electrónico no deseado (*spammer*) y tal vez ellos tienen una estación de radio pirata y están anunciando algo del espacio BGP [protocolo de pasarela de frontera] que no es suyo y realmente queremos asegurarnos de que cualquier respuesta que resultase en un registro A o un registro AAAA que esté dentro de ese espacio pirateado no se resuelva hoy.

Así que, volcar todos esos resultados de observación y análisis en la zona de política de respuesta, a la cual luego los servidores recursivos se suscriben.

Ahora, deseo señalar que esto es un acto voluntario. El operador del servidor recursivo tiene que desear que esto ocurra. Esta no es una SOPA [Ley de cese a la piratería en línea]. Esto no es algo que se le hace a usted por alguien de arriba y usted no puede evitarlo.

Además, si su servidor recursivo está suscribiendo a una de estas cosas y usted lo odia, entonces puede cambiar a 8.8.8.8, de modo que es muy voluntario, incluso para un resolutor stub. Por lo tanto, todo este método, aunque puede ser utilizado para intentar censurar, realmente no es para ello. Es... tiene que ser visto como un agregado de valor o no será utilizado por el operador del servidor recursivo o por el operador del resolutor stub.

Así que, quiero sacar eso también.

Entonces, ¿cuáles son los números? Un servidor recursivo dado puede estar ejecutando BIND [Dominio de Nombres de Internet de Berkeley] o Unbound, usando algún software que conozco o PowerDNS, o... hay un cuarto. Existen cuatro implementaciones independientes que no comparten ningún código fuente entre sí, y todas interactúan correctamente. Y en el mundo del IETF, si usted tiene múltiples implementaciones interactuantes, entonces usted puede comenzar a creer que tal vez el documento del protocolo está lo suficientemente completo. Así que, con cuatro, creo que tenemos eso cubierto.

Hay miles de servidores recursivos que se suscriben a una o más zonas de política de respuesta. Y hay una docena de proveedores de seguridad que publican sus observaciones y

análisis en este foro. Rod Rasmussen representa a uno o lo hizo hasta hace poco.

Pero hay un sitio web, dnsrpz.info, que tiene una lista de todas esas implementaciones, todos esos editores y tiene indicadores hacia la especificación. Y esto es lo que la comunidad está haciendo para protegerse en el extremo cercano de los problemas que se están introduciendo en aquel extremo donde no podemos evitarlos. Y está funcionando. Está funcionando muy bien.

Nosotros... mi empresa ahora ofrece una política de seguridad en este formato de zona, y ha sido bien recibida. Y creo que Rod tuvo un buen éxito con esto también, en su reciente compañía. Por lo tanto, es bueno para la industria de la seguridad, ya que nos da más clientes para nuestras cosas, y también es bueno para las personas que están tratando de defenderse porque les da un nuevo cuello de botella en su red y un estándar muy abierto que pueden tener una solución multivendor [sistema configurable para tener múltiples proveedores] en cuanto a qué conjunto de políticas de seguridad quieren suscribirse.

Por último, pero no menos importante, esta también es una solución empresarial. Así que, aunque mencioné que Rod y yo hemos estado en el negocio de vender estas políticas, también es muy común, digamos, que un banco tenga una lista de cosas

que no quieren resolver hoy. Y en ausencia de esta tecnología, han estado creando zonas vacías en cualquier punto del espacio de nombres donde desean esencialmente aplicar un poco de corrector líquido [*white-out*] y evitar que las cosas sean visibles. Y si usted está haciendo 6 millones de ellos y está teniendo una fuga de la mitad de todos los días, esa es una fuga muy importante en la configuración de su servidor de nombres. Mientras que, en algo como la zona de política de respuesta, no está cambiando su configuración del servidor de nombres. Sólo está cambiando la política de respuesta. Es una operación muy ligera.

Así que, inevitablemente, las personas que instalan esto, lo primero que hacen es crear una zona de política de respuesta local que es mantenida por su propio departamento de seguridad para que cuando se den cuenta de las amenazas... de nuevo, es una observación y análisis nuevamente... puedan de algún modo verter rápidamente la política de respuesta en su servidor de nombres recursivo, en una especie de forma similar a la de la matriz, donde se descarga en un lugar y de repente se sincroniza en todas partes y entonces la empresa ya no responde a ciertas preguntas o ya no responde a preguntas que producirían ciertas respuestas.

Otras políticas podrían ser, no responder nada que involucre a cierto nombre de servidor de nombres. Por lo tanto,

esencialmente se puede envenenar el contenido sin saber cuál es la pregunta o la respuesta; aunque sabe que si procede de ese nombre de servidor de nombres o de una dirección IP de un servidor de nombres que está en un cierto rango, entonces tiene que ser malo. Hay muchas perillas. Tal como David Conrad me dijo una vez, tenemos bastante soga para que cualquiera que quiera colgarse ahora pueda hacerlo.

Y supongo que lo último que hay que mencionar es que, mayormente, lo que hacemos es decir: "Quiero mentir" y pretender que algo que existe, no existe. En otras palabras, es una señal NXDOMAIN sintética, falsa. NXDOMAIN es el valor del código de retorno en el DNS que indica que la pregunta que está realizando se refiere a algo que no existe. Pero eso no es lo único que se puede hacer, ni mucho menos, porque mucha gente no quiere hacer eso. Crearían lo que se llama un jardín amurallado donde... digamos que usted busca un nombre Conficker, una botnet Conficker con un algoritmo para la generación de dominios. Podría ser que lo que realmente usted desea, es poner una ventana emergente (*pop-up*) en la pantalla de su usuario para decir: "Oiga, está siendo infectado con Conficker". Y, de hecho, usted puede hacer eso si usted apenas.... en lugar de contestar con un NXDOMAIN sintético, usted contesta con un alias sintético para decir que el nombre canónico de lo que usted está buscando es

jardinamurallado.ejemplo.com. De modo que es un servidor web que es administrado por la propia empresa con el fin de decirle a la gente: "Oiga, probablemente está infectado, debe llamar al departamento de IT [Tecnologías de la Información] ahora." Por lo tanto, hay muchas otras cosas que hacer además de mentir acerca de si algo existe.

Y supongo que realmente el último tema, antes de llegar a las preguntas y respuestas, es que estamos mintiendo. Son mentiras. Esto es... la autoridad es propiedad de alguien que usted considera es malicioso y usted no quiere la verdad. Y está decidiendo mentirse a sí mismo porque esa es la manera de conseguir que su red y sus activos respondan a una amenaza particular. Y al mentir, una de las cosas que se rompen son las DNSSEC. Y las DNSSEC son increíblemente importantes para el futuro de la economía mundial. Tenemos que tenerlas, no sólo para la DANE, sino para todas las otras aplicaciones que reconocen las DNSSEC, que están en preparación en varias etapas. Y esto rompe eso. Si ejecuta esto y los datos mismos fueron firmados por la autoridad, nuestro código lo ignorará. Nuestro código no ejercerá la política sobre los nombres firmados con las DNSSEC. Y eso da a los chicos malos una manera muy fácil de transitar todo esto, que es simplemente activar las DNSSEC.

Sin embargo, el resolutor stub también tendría que estar pidiendo las DNSSEC. De modo que aún no existe la ubicuidad suficiente para las DNSSEC a fin de evitar que esto sea eficaz. Pero en algún momento, eso va a ser un problema. Y espero que después de que publiquemos la especificación actual y pasemos el control del cambio al IETF, que va a ser casi inmediatamente un nuevo protocolo que es exactamente como este, salvo que hace algo un poco más sensible con las DNSSEC. Por lo tanto, esa es una debilidad conocida que no nos está afectando ahora. Pero realmente espero que nos afecte porque si nos afecta, eso significa que las DNSSEC se han hecho omnipresentes, que es lo que necesitamos. Esos son los comentarios que hemos preparado, y estoy listo para preguntas y respuestas. David, ¿cuántos minutos tenemos?

DAVID CONRAD: Probablemente tenemos cinco o siete minutos para hacer preguntas a Paul. ¿Quién desea comenzar?

¿No hay preguntas para Paul? Bien. Entonces, comenzaré yo.

[Risas]

Entonces Paul, supongo que una implicación de las cosas de RPZ [Zona de Política de Respuesta] es que de alguna manera refuerza los problemas que muchos de los nuevos gTLD están

teniendo con la aceptación universal. En primer lugar, ¿es preciso eso? Y, en segundo lugar, ¿hay alguna manera de abordarlo?

PAUL VIXIE: Así que, tengo un hijo que trabajó en la industria de nombres de dominio por un tiempo. Y así, cuando .ENTERPRISES se hizo disponible, él registró VIXIE.ENTERPRISES, que me pareció muy lindo porque yo tenía una empresa de consultoría antes de que él naciera.

Y luego procedió a intentar usarlo y descubrió que .ENTERPRISES no era justo uno de los patrones que, digamos, United Airlines esperaba que se asociaran con su cuenta. Ahora, afortunadamente, conocí al señor de United y pude arreglar eso. Pero él ha tenido todo tipo de problemas. Por lo tanto, entiendo totalmente que estos nuevos TLD genéricos son difíciles de usar porque mucha gente piensa, ya saben, podría ser .COM,. NET, .ORG, .INFO, o un montón de códigos de país. Y si no es eso, entonces tiene que ser un error de sintaxis. Así que, entiendo eso. Pero eso no viene de la RPZ, y no he oído hablar de ese problema en asociación con la RPZ.

DAVID CONRAD: Bien. Usted indicó que la RPZ no funciona con las DNSSEC. Mi suposición había sido que la RPZ trabajó con las DNSSEC en el sentido de que, si una zona fue firmada, la respuesta volvió para ser validada, podría ser validada. Y luego, después de la validación, la respuesta que fue devuelta al resolutor stub sería modificada según lo indicado apropiadamente por la RPZ.

PAUL VIXIE: Eso es casi cierto. Ciertamente va a funcionar de esa manera si el resolutor stub no está pidiendo las DNSSEC. Si no se establece D.O. igual a 1, entonces lo que acaba de decir es lo que va a pasar. Vamos a buscar los datos. Lo validaremos, si es posible. Lo pondremos en el caché. Y luego, cuando estemos intentando firmar una respuesta a la pregunta original, vamos a decir: espere, hay una política. Y el resolutor stub no pidió las DNSSEC, así que sólo vamos a... vamos a inventar cosas, porque si el resolutor stub no será capaz de decir que estamos mintiendo, entonces vamos a mentir. Sin embargo, si el resolutor stub está pidiendo registros del DNS y esos registros del DNS existen, no aplicaremos la política.

DAVID CONRAD: ¿George?

GEORGE SADOWSKY: Muchas gracias por lo refrescado en su presentación Paul. Estoy casi listo para tomar el examen.

Entonces, supongo que esto es más una pregunta con respecto a las personas que producen la información sobre la cual se basa la política.

Hablo acerca de las consideraciones del tiempo de vida útil aquí. ¿Con qué frecuencia hay que transmitir esto? ¿Qué frecuente es el cambio que desea darle a sus usuarios? ¿Cómo conoce cuál es ese tiempo de vida útil?

PAUL VIXIE: Bien. Así que, créanlo o no, me alegra que lo haya preguntado. De modo que la conexión es en vivo. Por lo tanto, si usted hace un cambio entonces, dado que esta es una zona del DNS normal, habrá una notificación y habrá una transferencia de zona incremental, y habrá actualizaciones casi instantáneas. Entonces, en la medida en que usted cambia de opinión y dice: guau, me gustó esa política hace diez minutos, pero no me gusta ahora, sólo puede cambiar su opinión y eso se reflejará instantáneamente a través de su base de suscripción. Es muy importante para nosotros no romper nada nuevo. De modo que con ese fin, si... no queríamos datos obsoletos en el sistema. Así que le daré un ejemplo.

Mi empresa vende un servicio de dominio recientemente observado. Eso es porque hemos observado que hay 2 1/2 nuevos puntos de delegación creados en Internet cada segundo, y probablemente la mitad de ellos se habrán ido en 24 horas. Y 1/6 de ellos se habrán ido en diez minutos. Hay una tasa de fuga muy alta. Estas cosas se crean con el propósito de molestar a alguien, y se bajan casi instantáneamente en muchos casos o son colocados en la lista negra por personas como SpamHaus. De modo que eso no significa que todo lo que es nuevo es malo, pero sí significa que hay una probabilidad estadística de que algo que es nuevo vaya a ser malo.

Desde que recuerdo, los buenos viejos días donde usted solicitaba un nombre de. COM, si era después de martes usted lo conseguía para el viernes; no me molesta que los nuevos nombres del dominio no trabajen del todo bien. Todo lo que la ICANN y su ecosistema han desarrollado, que lo hace bajar a 30 segundos, realmente no tiene un caso de uso no malicioso que me importase.

Por lo tanto, eso significa que tenemos que enviar una actualización una vez por segundo a nuestros suscriptores de RPZ diciendo: "Aquí están los nuevos nombres de dominio que hemos observado. Y, por cierto, ahora estamos eliminando los que tienen más de diez minutos de antigüedad porque sólo quieren los nuevos y no es nuevo uno luego de transcurridos

diez minutos, según su definición ". Tenemos diferentes definiciones.

Redes, el envío de una actualización una vez por segundo es capaz de sincronizar la política de respuesta a través de miles de clientes sintéticos o docenas de clientes reales. Y todo está funcionando. Así que esto es muy fluido. No hay nada obsoleto.

DAVID CONRAD: ¿Warren?

WARREN KUMARI: Así que supongo que esto es más un comentario que una pregunta. Entonces, yo solía ejecutar mi propio servidor de nombres para un montón de dominios, y luego me molestó mucho con la cantidad de spam, así que los apagué.

Y luego empecé a suscribirme a los feed [documentos que contienen información] de RPZ de un montón de diferentes personas, y los he vuelto a activar a todos de nuevo, porque con la RPZ, no tengo casi ningún spam con el cual lidiar, ¿correcto? Consigo los feed de spam a partir de puñado de gente con RPZ. Sólo se encarga de las cosas y ahora todo funciona de nuevo. Esto es...

PAUL VIXIE: Gracias por mencionarlo. Y permítame comentar sobre su comentario.

No se puede hacer el trabajo en Internet a menos que el DNS funcione. Sé que hay muchos protocolos peer-to-peer [entre pares] por ahí, y por lo tanto no todas las personas de BitTorrent se darían cuenta cuando el DNS no funciona. Pero para el resto de nosotros, si el DNS no funciona, no importa lo que es accesible porque no vamos a estar escribiendo direcciones de IP. Ciertamente no vamos a estar escribiendo direcciones IPv6.

Ahora, esa propiedad también funciona para los malos. No son sólo los buenos que no pueden hacer el trabajo si el DNS no está funcionando. Los chicos malos no pueden ser alcanzados si no están en el DNS.

Y para mí, usted ha mencionado el spam. Y así, para mí spam significa correo electrónico directamente, debido a cuando nací.

Tengo mi servidor de correo, es Postfix y está cableado para que intente hacer una búsqueda del DNS de cada nombre en el encabezado, cada nombre en el sobre, y cada nombre en el cuerpo del correo electrónico. Y si alguno de ellos falla, yo rechazo el correo, lo cual significa que al usar este cuello de botella sólo como un lugar para decir que estos nombres deberían ser inexistentes; si en realidad existen, entonces mentir y decir que no existen causará que ocurran diversas otras fallas

dentro de su infraestructura. Tiene que estar preparado para ellos. Puede ser un poco sorpresivo cuando no recibe ese spam. De hecho, lo que ha mencionado es una intención secundaria de todo este esfuerzo.

DAVID CONRAD: Bien. Gracias, Paul, por su presentación sobre la RPZ, y ahora pasamos a Paul Wouters.

PAUL WOUTERS: Gracias.

Dado que tengo la palabra, un pequeño comentario. Tengo que decir que Paul Vixie y John Gilmore son las dos personas más difíciles para enviarles un correo electrónico en el planeta, debido a su defensa o la falta de mecanismos de defensa que despliegan principalmente.

Así que, con eso...

>> (Fuera del micrófono.)

PAUL WOUTERS: Estoy feliz de los daños colaterales.

De modo que, el obtener a las DNSSEC desplegadas a gran escala, eso ha sido problemático. El registro DS [registro del segmento de datos] que la gente necesita para entrar en su zona principal, es un proceso muy difícil de atravesar e involucra a demasiados humanos, y el humano más importante está trabajando como registratario y él realmente no sabe nada. Acaba de comprar un servicio y un nombre de dominio y no sabe nada. Sólo quiere que funcione y tiene un operador de dominio que lo ejecuta todo, y por lo tanto no sabe ni qué son las DNSSEC y no sabe cómo habilitarlas, e incluso si su operador de DNS le dice qué hacer, realmente se le dificulta hacerlo.

De modo que hay una gran cantidad de dominios que en varios... proveedores de alojamiento muy grandes son, básicamente firmados pero no delegados con un registro DS por lo cual, a pesar de que son seguros por sí mismos, son como una pequeña isla porque hay... ese registro DS no entró en la zona principal, porque no hay manera de hacer eso.

Y así, ese problema necesitaba una solución.

Y el IETF primero evitó abordarlo, pero en algún momento, se convirtió en un problema demasiado grande, por lo que volvieron y ellos... ellos... eso es confuso. Cerraré mi computadora portátil.

Por lo tanto, las dos cosas que tenían que hacer... y esto se hace ahora en la RFC-8078 que se acaba de publicar la semana pasada, es de alguna manera contar con una forma en que el operador del DNS señale al Registro que este dominio ahora tiene un registro DS en él y pedir por favor si este registro DS puede ser publicado.

Y entonces la otra cosa que los operadores de DS también necesitan tener es una manera de decir: "Mi cliente se está alejando; mi cliente no quiere más las DNSSEC". Necesitamos alguna forma de decirle al Registro que elimine ese registro de nuevo, del mismo modo, cuando las DNSSEC ya no son necesarias.

De modo que esta RFC básicamente permite que uno haga eso. Lo que hace es que se crea... que utiliza el tiempo récord del CDS [servidor de entrega de contenido], que es básicamente el mismo tipo de registro exacto que un DS, pero que se publica en del lado del cliente, así en la propia zona del cliente.

Entonces, una vez que se publica allí, usted encuentra alguna forma de llegar a su Registro y decir: "Oiga, he publicado este registro CDS. Puede echarle un vistazo y si está de acuerdo entonces publicarlo como un registro DS en su zona principal."

De modo que eso es lo que hace este nuevo registro.

Disculpen. El registro no lo hace. El uso de esto aquí es nuevo.

Hay varias formas de cómo puede ponerse en contacto con su Registro, y eso se deja a otros borradores. Actualmente hay otro borrador que va a, como ejemplo, usar una interfaz restful [Transferencia de Estado Representativo] mediante el uso del HTTP [Protocolo de transferencia de hipertexto], para transmitir esa información, pero las personas podrían pensar en otros mecanismos para eso también. Y luego el registro de desactivación especial es el registro CDS con todos los ceros, lo cual básicamente significa: "Por favor, deshabilite esto, no queremos nada".

Y en realidad hay un error tipográfico en la diapositiva. Debe haber un cuarto cero, que también es un problema en la última revisión del borrador, pero lo encontramos a tiempo para la publicación de la RFC aunque, obviamente, no actualicé mi diapositiva.

Así que este sistema funciona. Debido a que también hay nuevas extensiones de EPP [Protocolo de Aprovisionamiento Extensible], el Registro —una vez que ha aceptado este tipo de actualización fuera del límite a partir del operador del DNS—, puede señalar esto de nuevo a su Registrador para que también sepa que este registro se ha actualizado y no ingresó a través de un flujo tradicional del EPP.

Y esto se está desplegando actualmente, o está en la... en la fase de despliegue para varios TLD y pronto esto significará que habrá cientos de miles de dominios más delegados, firmados con las DNSSEC, de modo que esto debería ser un gran salto en el despliegue de las DNSSEC y, sí, esperamos que sea un buen éxito.

DAVID CONRAD: Bien. ¿Alguna pregunta para Paul?

Sí Liman.

LARS JOHAN-LIMAN: Sólo un... Lars Liman aquí. Sólo una aclaración rápida. Estos son los registros CDS como fue propuesto por... ¿fue Olaf Kolkman? ¿O el que ha estado circulando en el IETF?

PAUL WOUTERS: Sí. Esta es la RFC de Olaf Kolkman, me refiero a que, sí.

LARS JOHAN-LIMAN: Correcto. Gracias. Y también, esto de algún modo coloca el enfoque sobre la falta de relación formal entre los operadores del DNS y los Registros, creo, que es bueno.

PAUL WOUTERS: No mencioné la palabra a propósito.

DAVID CONRAD: ¿Patrik?

PATRIK FÄLTSTRÖM: Han estado viendo a...

Aquí a su izquierda.

[Risas]

PATRIK FÄLTSTRÖM: Así que, lo que ha sucedido en el caso normal...si se puede volver a la diapositiva, por favor.

En el caso normal, la transacción DNSSEC se realiza a través del Registrador, de modo que el Registrador tiene plena responsabilidad final de asegurar que todo lo relacionado con el registratario esté completo, incluso la clave...el material clave.

En este caso, la actualización de la clave pasa desde el operador del DNS hasta el Registro sin pasar por el Registrador, ¿de acuerdo?

PAUL WOUTERS: Correcto.

PATRIK FÄLTSTRÖM: Y lo que usted está diciendo es que esto se activa a través de un evento en el EPP, ¿correcto?

Por lo tanto, el Registrador debe utilizar el comando pull [tirar o jalar] en ese caso para obtener la información sobre el nuevo material clave.

¿Es esa la intención?

Lo que me inquieta es que de repente el Registrador no tenga una visión completa de la... de la zona, lo cual cuestiona... lo cual podría tener un impacto sobre las responsabilidades del Registrador en relación con el Registro.

PAUL WOUTERS: Eso es correcto. Sí. Pero mi entendimiento era que había una nueva extensión de EPP que permite que el Registro empuje (push), así entonces el Registrador no necesita tirar (pull).

PATRIK FÄLTSTRÖM: Absolutamente. Hay extensiones donde se puede hacer eso. Pero hay... en el diseño normal del EPP, todo el diseño es para que los Registradores actualicen al Registro y no en la otra dirección.

PAUL WOUTERS: Correcto.

PATRIK FÄLTSTRÖM: Bien. Entonces esto es otra cosa donde el Registro está prescribiendo un cambio en la máquina de estado del Registrador, y tenemos muy, muy pocos de ellos y este es otro, ¿cierto?

PAUL WOUTERS: Correcto. Sin embargo, el Registrador también podría apoyar el mismo mecanismo y luego hacer que su registratario hable con ellos.

De modo que, para aquellos que están dispuestos a implementar todos los requisitos de las DNSSEC que no necesitan este trabajo alternativo, ellos no tendrían que hacer la máquina de estado. Es... siempre y cuando el Registrador y el operador del DNS tengan una buena relación de trabajo donde pueden hablar entre sí. Porque si el Registrador no puede hablar con el operador del DNS, entonces el problema sigue siendo que no pueden obtener esta información a menos que utilicen este mecanismo.

PATRIK FÄLTSTRÖM: Puedo hablarle como usando una consulta del DNS, ¿cierto?

De todos modos, por razones de transparencia, cuando examiné este documento, sugerí que este documento debería... debería normalizar este excelente registro CDS, independientemente si quien tira es el Registro o el Registrador.

PAUL WOUTERS: ¿Dónde publicaría esto el Registrador? ¿Se refiere a si el Registrador lo envía a través del EPP?

PATRIK FÄLTSTRÖM: No. Publicar...el... el Registrador está buscando el nuevo DS por parte del operador del DNS y lo empuja hacia el Registro usando el EPP.

PAUL WOUTERS: Ellos ya pueden hacer eso sin este borrador.

DAVID CONRAD: De modo que...

PATRIK FÄLTSTRÖM: Llevemos esto fuera de línea. Sí. Ya lo expliqué una vez en la lista de correo del IETF y probablemente no tenga que hacerlo aquí de nuevo.

DAVID CONRAD: Correcto. Dan y luego Warren.

DAN YORK: Entonces, yo sólo iba a decir gracias, Paul, por presentar esto, y creo que el punto clave, tal vez, para los miembros de la Junta Directiva de la ICANN y las otras personas que están escuchando aquí, que no quieren entrar en los detalles de algo de esto, esto es sólo para darse cuenta de que esto es parte de un trabajo en curso para brindar una mejor automatización en la forma en que funcionan las DNSSEC, porque ciertamente, cuando miramos a los despliegues de las DNSSEC a gran escala por parte de los operadores del DNS o de otras personas que buscan tratar de hacer esto, una de las grandes barreras que se identificó fue la obtención de esta información, estos registros DS, hasta los Registros.

De modo que este es uno de los mecanismos que ahora está disponible para los Registros que opten por hacer uso de esto, para ayudar con la automatización de esta publicación de información y hacer esto mejor, lo cual al final conducirá a un DNS más seguro.

Por lo tanto, este es... este es realmente el punto clave de esto, es un nuevo mecanismo que está disponible ahora, de modo que los Registros pueden ver esto como una manera de hacer que esto funcione.

Y para el punto de Patrik, los Registradores también podrían ver esto.

DAVID CONRAD: ¿Warren?

WARREN KUMARI: Así que la razón por la cual comencé a intentar interrumpir a Patrik es que las personas estaban hablando con objetivos contrapuestos.

Creo que también, Lars, mencionó que el proyecto originalmente era de Olaf. En realidad es Olafur, creo, fue el original... sí. Olafur y yo hicimos eso. Sí.

Entonces, el documento original no tenía la capacidad de que las personas dejen de publicar estos registros de manera automática. Había que pasar por el Registro o el Registrador, que creo que es de lo que Patrik estaba hablando. Específicamente dejamos un poco de lado el: "usted puede pasar por encima de su Registrador" debido a las mismas preocupaciones que Patrik estaba planteando. Esto se basa en ese borrador antiguo y añade nuevas características. O quizá yo también malentendí su...

PATRIK FÄLTSTRÖM: Lo que estoy tratando de hacer es separar la característica técnica, que es la capacidad del operador del DNS para señalar que este es un nuevo material clave, del posible impacto de la política con respecto a la relación entre el registratario, el Registrador y el Registro. Esa discusión es completamente diferente y podría ser complicada en ciertos TLD.

DAVID CONRAD: ¿Sólo una respuesta rápida? Sí.

>> Patrik, la cuestión fundamental que necesita ser resuelta es averiguar quién es el registratario, cuál es la forma de hablarle. Tenemos una cantidad limitada de Registros por lo que son convenientes como el punto de partida para hablar, pero si podemos de alguna manera entrar en RDAP [Protocolo de Acceso a los Datos de Registración de Nombres de Dominio] o algún otro protocolo, encontrar el identificador de la entidad dispuesta a hablar con nosotros, preferiblemente el Registro o un revendedor, incluso, o un revendedor de un revendedor, eso es lo que nadie puede encontrar hoy.

DAVID CONRAD: ¿Dmitry?

DMITRY KOHMANYUK: Hola. Sólo quiero hacer un comentario rápido de por qué la ventana del Registro está doble. Supongo que es un error tipográfico. En segundo lugar, probablemente secundaré el comentario de Patrik Faltstrom de que, sí, el modelo del EPP... y yo, por cierto, represento a uno de los TLD, ccTLD. Ejecutamos el EPP. Es Ucrania. Creo que el modelo en el cual el estado se divide es muy malo. También pienso que el modelo de tirar (pull) es muy malo y no se amplía. Sin embargo... y, sí, el EPP soporta las actualizaciones de DS, pero mi mayor problema aquí es que estamos tratando de separar el DNS... lo siento, el registro NS y la gestión de registros DS. Eso es malo. Debido a que el cambio de operador del DNS puede implicar tanto un cambio de registro DS y un cambio de registro del DNS. De alguna manera parece extraño que las actualizaciones de DS se supone que (indiscernible) este borrador sin la supervisión del registro del DNS.

Por lo tanto, yo diría que usted debería volver a la mesa de dibujo y ver cómo toda esta separación de Registrador, digamos, actualización de datos acerca de los nombres de la entidad, las direcciones y cosas en comparación con los datos técnicos. Sí, es una buena idea perder al operador técnico de terceros, pero el punto es la solución equivocada, además de la falta de relación contractual entre el operador del DNS, uno o

dos, y el Registro es la solución equivocada, y esa no es una manera de resolverlo y esa no es una forma de hacer que Internet sea más segura.

Así que, sí, buen intento, pero yo sólo...

PAUL WOUTERS: Bien, sólo voy... una nota muy rápida y luego se lo daré a Paul Vixie.

Ha habido una extensa discusión en el IETF sobre los disparadores versus temporizadores, y así que no lo repitamos otra vez.

Es una opción que los Registros pueden decidir escoger, y si algunos Registros no pueden hacerlo contractualmente o no desean hacerlo, está bien, pero esta va a ser una opción que es útil para una gran cantidad de personas que actualmente no pueden empujar los registros DS donde deben ir.

DMITRY KOHMANYUK: Bueno, sí. Hay muchas cuestiones. No creo que deberíamos discutirlas aquí ahora. Es mejor hacerlo en el entorno del IETF. Gracias.

PAUL WOUTERS: Bien.

DAVID CONRAD: ¿Paul?

PAUL VIXIE: Iba a ampliar ese punto. El NomCom trabaja arduamente para conseguir a las personas más calificadas que desean desempeñarse en esta junta, y no son necesariamente tan técnicos como la gente que utilizaba Internet en los años anteriores a que existiese la ICANN. Debemos usar su tiempo con sabiduría y respetar su tiempo, así que si pudieran por favor lanzar sus argumentos a un nivel que George Sadowsky pueda entender.

[Risas]

DAVID CONRAD: Y con eso, ahora estamos en cualquier otro asunto a tratar.

Ya saben, esto fue un intento para alguna forma de reestructurar la manera en que el TEG funciona. Hemos ofrecido reuniones de información de una a dos páginas a los miembros de la Junta Directiva antes de la reunión y nos preguntamos si eso sería beneficioso o si debiéramos continuar intentando evolucionar el TEG de una manera que lo haga más útil para los miembros de la Junta Directiva.

Y bien pueden decirlo ahora o pueden enviarme un correo electrónico o pueden hablar conmigo en el cóctel que está a punto de seguir. Los autobuses salen en unos 15 minutos. Y con eso, voy a cerrar esta sesión del TEG y les agradezco su participación.

[Aplausos]

[FIN DE LA TRANSCRIPCIÓN]