PRAGUE – ASO/NRO Presentation on RPKI
Wednesday, June 27, 2012 – 12:00 to 12:30
ICANN - Prague, Czech Republic

CHAIR DRYDEN: ¡Bienvenidos! El ASO y NRO ha habido varios intereses de miembros del GAC para que sepamos más sobre este tema y sé que es algo que la comunidad lo estaba trabajando, por eso le voy a pasar la palabra ahora al señor John Curen quien presentará asimismo y a sus colegas.

JOHN CURRAN: ¡Hola soy John Curran! Soy el presidente del NRO, la Organización de Curso De Número que también se desempeña como la organización de apoyo de ICANN para las direcciones. Tengo también junto a mi aquí en esta mesa al presidente de la organización de asesoramiento de nombre que se llama Louie Lee es un consejero, tenemos a los CEOs de las RIR que constituyen varias de estas organizaciones e incluyendo a mí mismo para, a Raúl Echeverría para LACNIC, a Paul Wilson para APNIC y a Adiel para AFRINIC.

También vamos a presentar cuestiones sobre el RPKI a Geoff Huston quien va a hablar a partir de ahora. ¡Gracias!

Geoff Huston: ¡Buenas tardes a todos! Esta presentación es muy técnica en cuanto cubre tecnologías que normalmente no usamos o no

estamos acostumbrados a ver usualmente. Se ocupa de tecnologías que se relacionan con la seguridad de nuestra infraestructura y nuestras comunicaciones.

Es interesante que haya muchas formas de ser malos en internet, hay muchas formas de hacer cosas malas. Ciertamente uno puede enviar mucho spam y puede tratar de corromper la operación del sistema del DNS y el DNS está bajo constantes ataques y uno puede también tratar de enviar paquetes muy particulares a ciertas maquinas para que las maquinas hagan cosas que nunca tendrían la intención de hacer. Y lo mismo ocurre con los virus porque los virus cambian la operación del sistema que infectan. Pero hay otros ataques que incluso son más molestos, esos ataques no intentan cambiar la operación de su máquina, sino que más bien como la maquina funcione bien, el ataque es más exitoso.

Estos dos tipos de ataques no se ocurren en maquinas individuales, sino en la infraestructura de internet en sí.

El primero ocurre en el Nombre De Dominio que es un tema con el cual muchos estamos muy familiarizados de hace muchos muchos años y los esfuerzos para presentar soluciones respecto de la seguridad del DNS. El DNSSEC y su implementación como vemos aquí en esta reunión de ICANN ya está en marcha, hay muchos talleres, mucha actividad y mucha comprensión.

El ruteo es diferente, el ruteo es un problema muy muy difícil. Para entender cómo redirigir esos paquetes al destino que tiene la intención de llegar, hay que utilizar algoritmos muy

sofisticados que se han establecido, el ruteo es un problema muy difícil incluso en términos de su tecnología subyacente.

Cuando nosotros construimos por primera vez los sistemas de ruteo y estoy volviendo alrededor de 40 años para atrás a la década de los años 60, esto se hizo en un entorno de investigación y el tomo de investigación tiene a pensar ciertas cosas muy básicas y una de esas cuestiones es que había ciertos jugadores. Todo el mundo tiene esas mismas suposiciones y los algoritmos están basados en la confianza mutua que es muy importante para internet.

La confianza mutua no es el entorno en el que vivimos, pero ¿cómo contrarrestar esta confianza mutua si no sepamos que todos son buenos jugadores? ¿Cuál es la respuesta?

La respuesta es que todos tienen que verificar todo y chequear todo, pero esa función de verificación es extraordinariamente difícil porque cada uno de los jugadores que rutea tiene que reunir mucha información todo el tiempo sobre direcciones y políticas de ruteo.

No existe un repositorio realizado de esa información ni tampoco técnicas bien entendidas a lo largo de todo internet, se trata de un trabajo muy difícil. Entonces en lugar de hacer esto, vamos a aplicar una solución que es eficiente en cuanto al costo y esta eficiencia en el costo significa que en el límite hay cosas un poco vaga, es decir hay cosas que suceden, el sistema es inseguro.

Ha habido muchos incidentes muy notables en el pasado, seguramente muchos de ustedes siguen en el área de seguridad y están conscientes de un incidente hace un par de años durante un par de horas en el que un ISP en el área de Asia logró bloquear el acceso al You Tube para un gran parte del planeta. Esto ocurre.

La mayoría de los incidentes que vemos son típicamente resultado del viaje de ciertos veos. A veces las cosas mandan mal y se propagan en el internet.

Pero las cuestiones de hoy son las vulnerabilidades de mañana. Es posible que haya cosas que se hagan por accidente y otras con intención. Tenemos que entender que el sistema en el que estamos trabajando no es bueno, ustedes van a ver que sus propios sistemas pueden ser perfectamente seguros o sus propios laptops pueden tener la mejor actualización y la web puede estar bien, todo funciona bien, pero si el sistema de ruteo esta en compromiso, los paquetes no van a ir al destino que tienen que llegar y pueden pasar por ciertos puntos no intencionados y navegar por un lugar al que no tienen que ir.

Obviamente no podemos mirar cada uno de los paquetes, los paquetes son demasiados, no podemos tener en cuenta toda por supuesto. Tampoco podemos equipar a los routeres con personas detrás de ello porque son muchas. Tenemos que buscar un sistema automatizado que opere a la misma velocidad que los paquetes que corren por ellos, lo que tenemos que poder hacer es colocar un discriminador en

nuestra infraestructura que nos permita detectar y excluir los intentos de colocar información falsa en el sistema de ruteo. Tenemos que poder distinguir lo bueno de lo malo automáticamente.

Hay muy pocas herramientas básicas que logran esto en un sistema público como cada una la criptografía les va a decir es fácil crear criptografías muy seguras de una sola vez, pero en internet no funciona así. Es fácil incluso crear sistema criptográfico cuando las dos partes van a intercambiar información y encontrarse antes para intercambiar secretos. Nosotros no tenemos este sistema, tenemos un sistema en que las partes que están tratando de intercambiar su información, nunca se han reunido y nunca se van a encontrar ni tampoco pueden encontrarse. Esto limita la posibilidad de las herramientas que tenemos a un conjunto muy pequeño y ese conjunto pequeño es el de la criptografía pública y privada.

Lo que estamos utilizando es en realidad, son reafirmas digitales convencionales que la firma precisamente una clave privada y solamente esa clave privada la puede desbloquear con un artefacto digital.

Lo siguiente es ¿cómo enviamos esas claves públicas a lo largo de la red? ¿Cómo distribuimos esas credenciales? ¿Como injectamos esa autoridad confiable dentro de la red?

Entonces tenemos que entender en primer lugar cómo describimos a la confianza. Yo tengo una dirección y mi dirección IP es un número lo cual es algo un poco raro 3,10,

1.000.020 ¿Cómo sabe el resto del mundo que es el número de esa dirección IP es válido? ¿Genuino? porque el internet tiene que trabajar de una forma única, tenemos un sistema que asigna de forma singular las direcciones individuales hacia el sistema. Es el marco de asignación de direcciones, esa jerarquía asigna la autoridad eniana, luego lo manda a los registros nacionales y quizás a otros registros locales hacia distintas maquinas.

Mi número entonces es único porque APINIC me lo dio y el número de APINIC es único porque IANA se lo dio a APINIC.

Si pudiéramos describir esa cadena, nos daría las credenciales para crear confianza en el sistema de direcciones, por eso lo que tratamos de hacer no es introducir nuevos datos, estamos tratando de re-formatear el registro para permitir que los mecanismos de autenticación sean construidos por encima de ellos.

Esto nos lleva luego al concepto de un certificado de recurso, un certificado es un artefacto bastante viejo en nuestro mundo. Hay certificados digitales el X509 que se refieren a varios años para atrás y estamos hablando de un estándar bastante común.

Es un documento digital que básicamente reúne recursos de número y una clave pública y las claves privadas con los certificados. Entonces se trata de un artefacto que puede validar y firmar algo, es decir esta dirección es mía cualquier de ustedes va a poder darse cuenta si estoy online o no, es decir si

estoy mintiendo o no. Ustedes van a poder autenticar mi afirmación.

Creo que estoy bastante poderoso y ciertamente diría que no es algo que RIR inventó por sí mismo, sino que estábamos trabajando en ese espacio en conjunto como el RIRs y dentro de la fuerza del trabajo de ingeniero internet desde el año 2006 para generar una tecnología viable y estándares que luego permitan construir y operar de forma adecuada, un enfoque que va hacia adelante.

Esta es una forma de publicar los mismos datos que siempre publicamos, es un formato que es diferente porque ahora estos certificados X.509 son precisamente de este tipo de certificado y los que lo tienen pueden optar por generar un certificado digital que dice que su parte clave está asociado singularmente con las distintas direcciones de IP, y se deriva directamente de la base de datos de registración subyacente, por lo tanto esas bases refleja la misma información.

Entonces ahora tenemos este concepto y es como la jerarquía del nombre de dominio, se trata de una jerarquía de certificados digitales que es conocida dentro del mundo de seguridad porque a ellas les encanta crear términos nuevos, siempre usan un término nuevo cuando un término viejo no podría funcionar perfectamente. Entonces en vez de utilizar la palabra “jerarquía”, a ellos les gusta “Infraestructura De Clave Pública”, PKI.

Esta es una jerarquía de certificado que habla no solamente de mi identidad, no de mi role, no de la cuestión de lo que conversonamente hablar los certificados, sino se trata de una jerarquía que habla sobre los recursos numéricos de IP y esto permite declaraciones como que yo soy el titular de una dirección en particular y que esa dirección puede ser firmada digitalmente para cualquier otra persona y cualquier otro puede verificar si esa afirmación es verdadera o falsa.

Cuando me refiero a cualquier persona, realmente estoy diciendo cualquier persona o cualquier cosa incluso cualquier router. Cualquier elemento de switching dentro de la red y hasta incluso cualquier interface de comande y control para el soporte operativo de la red porque se puede decir cosas que se relacionan directamente con cómo las direcciones de internet son originales y routeadas. Yo, Geoff, el propietario de 1.1.0/24 – y lo soy – puedo autorizar AS23456 y solo esa red va a routearse hacia mí. El corolario es que si cualquier persona intenta atacar mi dirección, no solamente yo, o sea voy a saber que están metiendo pero cualquier otra persona en la sala y cualquier otra persona en internet ellos también van a saber que están metiendo.es mucho más difícil mentir cuando uno sabe que están metiendo.

Este es un nuevo desarrollo para nosotros. La seguridad es muy difícil para nosotros y la comunidad ha tenido largos debates a medidas que vamos avanzando. Somos conscientes que en varios regímenes ha habido certificados digitales y ha habido interés en que los regímenes digitales revoquen los certificados

digitales. La comunidad tiene discusiones en torno al terma de ser obligados por un tribunal a revocar o alterar un certificado. No tenemos ninguna respuesta para esto, pero observamos el mismo proceso judicial que podría dirigir a un propietario de un registro muy fácilmente a cambiar el contenido del registro. Revocar un certificado, cambiar el contenido del registro es más o menos lo mismo. Por eso decimos que no tenemos una solución pero tampoco presentado ni reducido los factores en torno a este tema de las presiones externas sobre la integridad de la totalidad del sistema de registro.

Es una jerarquía como el DNS. Y si uno no logra comprometer la raíz, el efecto influye hacia otras partes de la infraestructura. Y si se compromete muy alto en esa jerarquía, los daños y los riesgos potenciales son muy grandes. Pero esto es similar a comprometer los certificados que utilizan Visa o MasterCard. Si ustedes piensan en el caos, imagínense qué ocurriría si se comprometen. Muchos de los sistemas digitales de la actualidad que tienen que ver con gran parte de nuestra economía tienen los mismos problemas. La industria ha generado muchos estándares para asegurar la integridad de la operación de los certificados. Estándares FIPS que tratan de generar las claves para que los logremos. Utilizamos estas claves y no podemos hacerlo mejor, pero ciertamente tratamos de hacer lo mejor que podamos. Nuestros sistemas de gestión de claves, nuestros certificados están al tope de los estándares de industria en este sentido.

También hay un tema en cuanto a la flexibilidad, muestro muchos sistemas que tienen modo prueba de fallos, pero el sistema actual particularmente en el área de la publicación de políticas confía en la existencia de un lugar único en el que esas políticas están alojadas y es la forma en la que se realiza lo que le da la integridad. Los datos firmados son diferentes. Si están firmados, todos pueden publicarlos y cualquier persona que reciba cualquier copia puede inmediatamente decir si es una copia confiable del original porque digitalmente no se puede distinguir. Cada uno de vosotros pueden tomar una copia y republicarla y cualquiera que tome o se ha republicado puede asegurar que es exactamente igual que el original bit por bit. Entonces, sí, hay cuestiones de fracaso, pero al mismo tiempo esta información firmada nosotros consideramos que es mucho más flexible dentro de la infraestructura.

Siguiente diapositiva ¡por favor!

¿Entonces dónde estamos ahora? Estamos muy avanzados en este proceso porque el sistema de ruteo tiene vulnerabilidad y el sistema de los nombres de dominios de internet es importante y estamos tratando de ganar velocidad. En cuanto a la infraestructura de certificados, muchos registros regionales han tratado incorporar esto en su sistema de producción. Los miembros dentro de esta comunidad en particular pueden generar los certificados según deseen desde ahora.los RIR siguen trabajando con las comunidades para completar sus implementaciones. Hay mucho trabajo especializado y hay muchas diferencias en la implementación. Por lo tanto algunos

RIRs están haciendo las cosas útilmente diferentes, pero los resultados se verán en el futuro cercano. Pero estamos embarcados en esta reproducción y quisiéramos que todos estos registros regionales, los RIRs, terminaran esto rápidamente.

Los certificados no son todo. Hay que integrarlos a los sistemas operativos actuales. Tenemos que tener Apps (aplicaciones). Y como otros sistemas. Estamos trabajando mucho no solamente con los RIRs, sino también con IETF y con otros organismos públicos para generar modulas de plug-in para esto. También tenemos que distribuir y sincronizar esta información sobre la validez de toda la dirección y de toda ruta en internet en todos los momentos para asegurarnos de que estos datos sean completos y sean exactos todo el tiempo.

Al mismo tiempo IETF, hay un trabajo en curso para asegurar el protocolo del rutamiento específico PGP. Y estamos avanzando. Ya he resuelto algunos temas relacionados con la integridad de sesiones y la integridad de la oxigenación. Pero ahora estamos viendo que tenemos un problema de encadenamiento que nos lleva a tomarnos una pausa para pensar, pero todos somos muy optimistas que entre la curva de tecnología de la ley de Moore, uno es más eficiente que el logaritmo de encriptación y un conocimiento o una práctica más común de la criptografía en nuestra comunidad vamos a poder resolver estos temas como se han resuelto otros.

Así que creemos que esto lo vamos a poder lograr en el futuro cercano.

Bueno pasamos a la próxima diapositiva.

Creo que ya he cubierto todo lo que quería comentarles y con gusto les pueda responder a cualquier pregunta que tengan. ¡Gracias!

CHAIR DRYDEN: ¡Muchas gracias! Veo que Nueva Zelanda pidió la palabra.

Nueva Zelanda: ¡Gracias! Ésta ha sido una presentación muy interesante. Creo que la pregunta obvia para el GAC es ¿hay alguna política pública o algún impedimento en términos de política pública para lograr esto? ¿Algo que el GAC pueda hacer para acelerar la implementación de estos protocolos? ¡Gracias!

Geoff Huston: Ciertamente algunos organismos internacionales han estado muy conscientes de la naturaleza de estos problemas y han sido muy activos al apoyar la investigación del desarrollo de algunos organismos de Estados Unidos, han trabajando en este ámbito por muchos años pero no son las únicas en el único país. Hemos visto muchos otros países que son conscientes del problema y que apoyan actividades en este sentido, o sea aquello es bueno.

Tenemos este tema que no operamos bajo los términos y condiciones de la inmunidad de un ámbito legislativo y judicial. Entonces se ven los certificados en las comunidades expresan su preocupación de que un tribunal diga que se tiene que revocar un certificado porque las implicancias de esa revocación no es que simplemente no van a tener esa dirección, sino que los certificados de la dirección para el enrutamiento también desaparecen. Esto saca la validez de la presencia de esa dirección y que esto desaparece para todos los demás.

Y al introducir la seguridad, también se introducen estos otros factores que son novedosos en algunos casos. No estoy seguro de tener todas las respuestas, no sé si estoy buscando respuestas en este momento, pero entre las cosas que tenemos que hablar en un foro de política pública ciertamente esta es una de ellas.

CHAIR DRYDEN: ¡Muchas gracias! John querías responder también y veo que Paul tiene la palabra también.

JOHN CURRAN: Con respecto a alentar esta implementación, es importante recordar que la decisión de proveedores de servicio de utilizar la PKI y de tener seguridad en su información de enrutamiento o de su política de enrutamiento, su punto es algo voluntario. Los proveedores de servicio deciden que van a participar en esta infraestructura RPKI porque al hacerlo, la información de

enrutamiento se ve menos comprometida con otros. De la misma manera deciden prestar atención a la información de RPKI porque cuando reciben la información de enrutamiento, van a tener o recibir información sospechosa o incorrecta de enrutamiento, entonces muchos utilizan nuestra RPKI y prestan atención a los datos recibidos pero para los proveedores todo esto se basa en una decisión voluntaria. En la región de ARIN tenemos Canadá, Estados Unidos y 26 economías del Caribe y soy consciente que en Estados Unidos hay grupos de confiabilidad de internet, hay un grupo de mejores prácticas patrocinados por la FCC que hace referencia a las mejores prácticas en la seguridad en el enrutamiento.

Entonces hay maneras de ver todo esto, pero esto no es algo que los RIRs exigen que se haga. Somos una ubicación natural para proporcionar la infraestructura para esto, pero el uso de esto tanto a la publicación como en la observación de los datos recibidos tiene que ver con la decisión voluntaria de los ISP.

CHAIR DRYDEN: ¡Gracias! ¿Paul querías añadir algo?

PAUL WILSON: John cubrió muy bien. Otros temas que tal vez debemos recordar para ver el sistema actual como uno en el que los RIRs ofrecen los detalles de registración de las direcciones que nosotros hemos asignado. Los certificados en cierta forma, la medida en que tienen una firma con los mismos registros se

manejan de la misma manera que un email con una firma digital que indica que viene del origen del que firma el email. José John se refirió a este proceso, que es importante considerar lo que el proveedor decide hacer a través de una opt-in, ¿no? de la opción de participar. Es decir ver qué pasa en una mitad de la ecuación y por otro lado también ver qué es lo que pasa con aquellos datos que recibe. Esto es un sistema que está evolucionado de manera totalmente compatible con el proceso consensuado de nuestro sistema de los RIRs que es ascendente en lugar de ser impuesto de los niveles más altos a las bases.

El hecho por el que estamos aquí haciendo esta presentación, es que nosotros sentimos que nuestro sistema ha estado en desarrollo durante muchos años a través de este proceso y que los RIRs también han hecho su proceso durante varios años y que las preguntas sobre el sistema comenzaron a propagarse ahora más ampliamente y pensamos que era útil para que el GAC tuviera también esta perspectiva, esta actualización con respecto a cómo funciona el sistema y para asegurarnos de que haya un entendimiento común.

Bueno referencia a esta opción de participar en este sistema de Opt-in que describimos acá y la diferencia a lo que se hacía en el pasado.

CHAIR DRYDEN: ¡Muchas gracias Paul! Tengo a Portugal, Noruega, Malasia y la Comisión Europea. Portugal por favor.

PORTUGAL: ¡Muchas gracias por la claridad en esta presentación! Es un tema sumamente técnico y lo presentaron de una manera que lo podíamos entender.

Sabia de los esfuerzos del sistema de RIPE. Ahora mi pregunta tiene que ver con algo que ya mencionó Nueva Zelanda teniendo en cuenta el papel del GAC. Sería interesante saber qué es lo que piensan ustedes que son cosas que podríamos hacer desde el punto de vista del asesoramiento que está relacionado a la junta cualquier otra cosa que les parezca que les podamos hacer para ser claro, no sé cómo, pero desde el punto de vista de la probación políticas a nivel nacional o simplemente a generar consciencia. Sería bueno si pudieran dejar en claro ¿qué pueden aportar los gobiernos en este sentido? ¡Gracias!

CHAIR DRYDEN: ¡Gracias Portugal! Toma la palabra Raúl.

RAUL ECHEBERRIA: ¡Gracias señora presidente! El objetivo por el que estamos aquí hablando de este tema con el GAC es que queremos comentarles qué es lo que estamos haciendo para que el gobierno esté al tanto de ello. Creo que es un cambio importante para el internet. Es un proyecto como dijo Geoff que lleva ya muchos años de trabajo y se ha hecho una gran inversión en términos de tiempo, trabajo, dinero; o sea es un

cabio grande para internet y es importante que los gobiernos lo conozcan. Probablemente creo que esa es la manera más importante o es la manera principal en la que nos pueden ayudar si es lo que quieren hacer, ¿no? Y generar conciencia- nos pueden ayudar generando conciencia en las industrias locales como dijo John por ejemplo. Tenemos un caso ilustrativo en Estados Unidos y esto también se puede hacer en otros países.

CHAIR DRYDEN: ¡Gracias Raúl! Tengo a Noruega, Malasia, Comisión Europea, Uruguay y El Reino Unido.

NORWAY: ¡Muchas gracias señora presidente! Muchas gracias Jeoff por esta actualización. Y por toda esta información tan valiosa que nos han brindado. Creo que es más importante para nosotros como gobiernos saber qué pasa con este sistema porque se toman medidas de seguridad muy importantes por internet.

Y también quería comentar alguna de las preguntas o de las cuestiones que tienen que ver con las políticas públicas. Creo que este tema que tratamos aquí nos lleva a pensar que podemos crear consciencia y también propiciar las mejores prácticas en las regiones y con reglamentación en distintas partes en Europa de la cual pertenece Noruega, tenemos facultades como inter-reguladores para establecer medidas de

seguridad para los proveedores del servicio de internet en caso de que concederemos que eso es lo adecuado hacer.

O sea que allí podemos trabajar en Noruega de esa manera. Podemos establecer este mandato para los ISPs noruegos. Pero también queremos que esto pueda conformarse en una mejor práctica entre los ISPs del mundo con internet. No se pueden aplicar medidas en forma aislada porque esto es un sistema mundial. O sea es importante verlo de esa perspectiva.

Una pregunta de índole técnica. En realidad son 2 preguntas, una más técnica y otra que tiene más que ver con los plazos. ¿Cuándo el sistema va a estar operativo? ¿Cuándo las aplicaciones y las enrutadores, todo va estar ya listo? y ¿cuándo se va a ser la estandarización para tener esto ya implementado y finalizado?

Otra pregunta que tiene que ver con el certificado. Los RIRs van a tener un certificado firmado que van a poder utilizar para firmar los recursos porque hay algunas inquietudes, es parte de algunos gobiernos y no del nuestro en particular, pero de otros gobiernos. Es que si los RIRs van a tener certificados formados y van a ser controlados por otra parte que esto tal vez pueda en caso de que se revoque ese certificado, se pueda arruinar todo el enrutamiento en internet, entonces me interesa saber cómo se va a construir esta cadena de confianza dentro del sistema del RPKI.

CHAIR DRYDEN: ¡Gracias Noruega! Geoff quiere responder.

GEOFF HUSTON: Voy a decir unas palabras y luego se lo paso a John el micrófono.

Cuando se habla de mejores prácticas en contraposición con un requisito regulatorio para la implementación y el use de ese tipo de tecnología, es cierto que el DNSSEC si yo tengo geoff.potaroo.net te lo firme o no ese relevante a menos que potaroo.net este firmado porque esto es lo importante en DNSSEC que llegar a ese nivel de raíz. Pero nuestro sistema de enrutamiento no tenemos las facilidades de establecer una jerarquía en el enrutamiento. Si nosotros tenemos asegurado BGP y luego pasamos esa información de enrutamiento, una sección de internet que no implementa esa forma de BGP, toda la información se pierde y cuando llegamos a otro lugar que sí lo poya eso no va a llegar allí. Entonces BGP es un protocolo que nos pueda dar una gran cantidad de beneficio.

Es uno de esos sistemas que si todos utilizáramos, daría un beneficio a nivel universal si se hacen partes, tenemos que ver quién se puede beneficiar, a quién puede afectar desde el punto de vista del enrutamiento porque este beneficio se ve reducido sobre manera, entonces hay que pensar cuidadosamente este tema de qué es una mejor practica de seguridad de la infraestructura a nivel nacional y regional. Hay que pensar con cuidado como ampliar al máximo esto y al mismo tiempo no imponer costo prohibitivo de altos riesgos al entorno operativo.

Entonces no estoy diciendo que es una respuesta clara. Ciertamente estos partes de una agenda en un proceso de política pública a nivel nacional que tiene que tratar como que se hace la implementación por partes en forma aislada y la tecnología porque esto no es tan beneficioso como una implementación a nivel universal.

CHAIR DRYDEN: John sugeriría que tal vez podríamos hablar un poquito de BGP y ponernos un texto, pero no todo el mundo conoce estas normas.

JOHN CURRAN: Ah, bueno. Soy John Curran. Voy a tomar las otras tres preguntas implícitas que estaban dentro de esa pregunta explicita.

En primer lugar quiero decir que con respecto a los tiempos, cada uno de los RIRs tiene su propio cronograma de implementación y esto es para la estructura y para los certificados digitales ya sea la emisión o la vinculación a los proveedores de servicios. En ese caso tenemos un cronograma otro RIR está mucho basada y adelantada que ARIN. Y la manera en que funciona las responsabilidades en nuestra región es tal que tenemos que tener muchos recaudos para asegurarnos de asociar nuestras actividades de firma digital con todas las organizaciones de manera que no haya un repudio.es decir que podamos confirmar que el ISP realmente solicito los

certificados. Esto requiere más trabajo de nuestra parte. Entonces nosotros tal vez somos los más rezagados y estamos pensando entre ahora y fines del próximo año para tener este servicio ya en producción. Creo que la mayoría de los otros registros regionales ya tienen los servicios listos hoy o sea es un tiempo mucho menor. Con respecto a los certificados que utiliza los RIRs y el anclaje que llamamos el ancla de confianza. Hay mucha información para establecer un elemento digital en los sistemas que dé confianza.

Si hablamos de varios ruteadores y son ISPs, pueden configurar cada uno en los cincos RIRs con esa ancla y de esa manera ustedes allí piensan que las cosa se emitieron en esos 5 RIRs y en todo lo que está debajo de esto. También es cierto que sería conveniente tener una única ancla de confianza global y que la IETF podría emitir esto junto con RIR.

Nosotros nos vamos a reunir con el equipo de Elise Gerich y esto pueda ser factible. Entonces en este caso vamos a tener la posibilidad de utilizar nuestra RPKI no con 5 anclas, sino con una única ancla global que utiliza los recursos de los 5 RIRs además de otros recursos, recursos reservados, recursos de direcciones de IP destinados a usos específicos. Lo bueno es que esto se pueda configurar en forma individual, o sea que una parte depende de una sola ancla de un RIR puede activarlo de esa manera o no.

Escuché que hablaron de regulación y cómo esto puede ayudar. Hay un paso antes de llegar a la regulación desde el punto de vista de la influencia y de la incidencia.

Muchos gobiernos son usuarios de la tecnología ICT. Ustedes tienen sus propias redes y sus propios sistemas porque ustedes quieren proveedores de servicios que tengan un rutamiento seguro y como clientes deberían pedirles que lo hagan. Esa es una buena forma de distribuir el interés o divulgar el interés en estas implementaciones y estas tecnologías.

No quiero emitir este paso intermedio donde ustedes como usuarios de las ICT, puedan también demandar calidades de proveedores de servicios, pidiendo que no utilizan un enrutamiento seguro ¡Gracias!

CHAIR DRYDEN: ¡Gracias! Doy la palabra a Malasia

MALASIA: ¡Gracias presidente! ¡Gracias por presentarnos esta tecnología! Quisiera decir que en este momento tenemos muchos desafíos para promover el DNSSEC para nuestros ISPs. A pesar de que nos regulamos, nosotros queremos que se ofrezcan como voluntarios porque esto es voluntario y ustedes deben entender que la actualización es muy lenta.

Me interesan mucho los plazos y los programas de extensión para que podamos promover estas tecnologías en nuestros países y a nuestros ISPs ¡Gracias!

CHAIR DRYDEN: Adiel ¿quisieras responder?

ADIEL AKPLOGAN: En cuanto a los plazos, todos estamos trabajando en conjunto para poder tener los mismos plazos y avanzar en este sentido.

Estamos pensando en lanzar la plataforma para que existan los certificados y que se puedan firmar. Y entonces el sistema ya está en marcha, ya se puede usar. El objetivo me parece y la presentación hoy es generar una consciencia para el GAC de manera que puedan ustedes generar la misma consciencia localmente y que se empieza a usar el sistema.

También tenemos un buen enfoque de los proveedores que tienen integrada esta tecnología en el IOS, de una manera que se pueda usar en el mundo real de internet hoy.

La actualización por supuesto va a ser muy lenta, pero ya está allí y seguramente vamos a empezar hacer que la gente lo utilice también.

CHAIR DRYDEN: ¡Gracias por la respuesta! Tenemos a la comisión europea, Uruguay, El Reino Unido y luego vamos a cerrar la sesión. Entonces Comisión Europea.

Comisión Europea: ¡Gracias señora presidente! Quisiera agradecer también a los presentadores nos solamente por estar aquí hablando sobre una tecnología muy importante, sino también hacer que esa tecnología sea entendible para todos. Entendemos que no es una tarea fácil y por eso le agradecemos.

Tengo 2 preguntas que puedan ser respondidas por cualquiera de ustedes que la quiera responder. En cuanto a las anclas de la confianza, ¿solamente nos referimos a los registros de internet o a otros también que puedan ser anclas confiables en el sistema?

Hay un requisito especial para que la identidad pueda brindar este servicio y ser un ancla confiable en los operadores.

La segunda pregunta: al principio de la presentación se mencionó esto, por eso quizás no lo he entendido o recordado , pero en cierto punto escuché alguien, creo que era Huston que se refería al hecho de que la comunidad tiene inquietudes respecto de que se tome una decisión que implique la revocación del certificado digital utilizando el sistema de RPKI.

Quisiera saber si pueden ustedes explicar qué partes de la comunidad están teniendo esta duda o estas inquietudes y si es que había casos de rechazo o esto se podría suceder en el corto plazo. Como Comisión Europea, no vamos a hacer ningún comentario sobre lo que hacen o no hacen las comunidades locales porque no es nuestro trabajo, pero queremos saber si esto ya sucede o si es una inquietud hipotética como aquellas inquietudes que nosotros como autoridades públicas, generalmente acusamos de poner sobre la mesa por eso, les agradezco la declaración.

GEOFF HUSTON: ¿Quién puede ser ancla confiable? Vamos a volver un poco para atrás y hagan una pregunta básica. ¿Quién puede emitir certificados que demuestren que alguna de las partes tiene un recurso o es titular de un recurso? En teoría, cualquier persona pueda hacerlo, ¿pero a quién hay que creerle?

La parte que emitió los recursos, quizás la mejor parte es la que puede emitir el certificado. Por eso, si APNIC genera un bloque de direcciones hacia un registro de internet local, entonces el certificado que emite APNIC es el certificado en el que hay que confiar y hay otra parte digital que es la emisión de certificado que emite otro que no se deber confiar. Entonces el modelo de confianza ha sido aliñado precisamente con el modelo de asignación de direcciones y en la medida en que haya sistemas seguros, las personas que lo usan, van a poder elegir cualquiera de los modelos de confianza que quieran, ciertamente nosotros

vamos a recomendar que utilizan el conjunto de confianza que corresponde a las agencias que asignan los recursos en primer lugar.

Ya sea que se trate de un conjunto de confianza de materiales emitido por cualquiera de los cinco RIRs y son 5 modelos de confianza o que uno utiliza una entidad de confianza para describir la raíz IANA y eso depende de ustedes, pero quizás no sería inteligente replicar lo que nosotros hicimos en los navegadores porque tuvimos más de 100 entidades. Y en este caso son demasiado. Entonces quizás un número menor es mejor, pero no tiene que ser uno sólo. En cuanto a la segunda pregunta sobre la discusión de las inquietudes, creo que hay que informar estas inquietudes tenían más que ver con el área europea y que allí se deben discutir en los foros adecuados. Lamentablemente Axel no está aquí, pero hubo instancias en que en un esparzo diferente.

Por razones diferentes hubo órdenes de revocación de certificados por otros objetivos que tuvieron los tribunales.

Y entonces podemos aplicar también esto a certificados digitales, quisiéramos pensar que no porque los certificados son un espejo del contenido de registros subyacente y revocaron certificados no cambian el registro per ce, pero lo hace más difícil. Y no estoy seguro si esta fue la intención de estos procesos.

Ciertamente a mi me gustaría pensar qué medida que avanzamos en este proceso y intentemos mas sobre la

integración de los certificados y de la criptografía digital en este infraestructura. El riesgo de que la sociedad es la sustituciones y de las herramientas funcionen con esto y agradezcan sus propios roles y responsabilidades respecto a esto. La revocación no va a ayudar para nada ¡Gracias!

CHAIR DRYDEN: ¡Gracias Geoff! Ahora tiene la palabra Uruguay.

URUGUAY: ¡Gracias por la interacción!

No sé si la perdí, pero quisiera entender cómo esta infraestructura se relaciona con la infraestructura nacional pública, no solo en cuanto al punto de vista técnico, sino también el punto de vista legal. Ustedes saben que en cada país el valor legal de un certificado y de la confianza del sistema de la infraestructura se relaciona con partes con autoridades certificación que tienen el poder de emitir los certificados por una identidad regulatoria, es decir que la infraestructura pública nacional está vinculada con algún tipo de adecuación y quiero saber cómo se relaciona esto, es decir si existe algún tipo de compatibilidad o no.

JOHN CURRAN: Usted está hacienda una pregunta legal y yo no soy abogado. Habiendo dicho eso en el proceso de explorar los aspectos de brindar certificados de RPKI, pareciera ser que cada país tiene

su propio marco para la validez legal de un documento firmado legal de un documento firmado digitalmente. Esto significa que los RIRs , al emitir estos certificados, nosotros aseguramos que de qué se sepa el significado de este certificado, es decir que estamos hablando del poseedor de un recurso y qué es lo que considera ese poseedor, es decir cuál considera que es la identidad que puede rutear este bloque de direcciones.

Por eso en algunos países sé que hay judiciales nacionales que hacen estos certificados y que los hacen equivalentes a documentos firmados emitidos por el registro.

Esto tiene implicaciones para los registros que emiten estos documentos y ocasiona que todos nosotros tengamos mucho cuidado al hacer correr estos certificados. Pero esto es una situación que se genera país por país, no puedo dar una respuesta general. Sin embargo puedo decir que los proveedores en los países que emiten estos certificados, tienen que poder entender que quizás están emitiendo documentos con la misma fortaleza legal.

URUGUAY: Si el ISP tiene alguna responsabilidad legal por cometer un delito como el ISP, el marco legal en el que estamos trabajando es el marco nacional y este marco legal está regulado por estas leyes nacionales y estas leyes nacionales tienen su infraestructura nacional.

Para una entonces de las preguntas ¿Qué puede hacer el GAC para tratar de resolver esto? quizás tener cierta compatibilidad entre los marcos nacionales y esto para poder brindar un sustento legal al trabajo con los ISPs a nivel local. Pero creo que tenemos que tener más información de ustedes para saber cómo trabajar a nuestros propios países.

JOHN CURRAN: Estoy de acuerdo.

CHAIR DRYDEN: Raul por favor.

RAUL ECHEBERRIA: En cuanto a añadir algunos elementos, es una infraestructura separada. Los certificados que son emitidos con este marco, tienen el único objetivo de ser utilizado para el enrutamiento de manera que no va a dar ninguna transacción en el uso de estos certificados. Los ISPs no van a utilizar estos certificados para hacer transacciones de ningún tipo a nivel local y por eso no va a dar ninguna responsabilidad legal en este sentido, van a usar esta información solamente para saber si la red que están anunciando un bloque de direcciones de internet es el que tiene la autoridad para hacerlo o no. Va a permitir que se tome una decisión sobre el enrutamiento nada más que eso.

Por eso estos certificados no se van a usar en ningún país para ningún objetivo que está regulado bajo el marco legal de cada uno de los países. No sé si esto responde a su pregunta.

URUGUAY: En el caso de que el ISP no utilice correctamente del enrutador para usar la red digamos.

GEOFF HUSTON: Hay muchos tipos de certificados, algunos se utilizan en el sistema de nombres de dominio para los sitios web http y otros se utilizan para demostrar la identidad de los ciudadanos de un país.

Convencionalmente nos encontramos con que los certificados que tienen un interés nacional regulatorio, son certificados que demuestran la identidad y el role de la gente, pero los certificados pueden hacer mucho más que eso a los que nosotros trabajamos, son mucho más similares a los que usan en el sistema de nombres de dominio en cuanto a la asociación de un nombre de dominio con una dirección IP para los sitio webs seguros.

Convencionalmente estos certificados que caen directamente en el marco regulatorio legal per se en forma convencional en muchos marcos tienen más vinculación con las practicas nacionales de la industria. Diría que estos certificados que no demuestran la identidad y no demuestran el role pero que asocian un par de claves, tienen una reflexión de artefacto técnico que es distinto de un role.

Y por lo tanto tienen más que ver con el área regulatoria que habla sobre los artefactos técnicos y de las cuestiones técnicas

como los certificados de nombres de dominio los cuales son distintos de los certificados de role o de identidad.

Por eso no veo el nivel de interés regulatorio en este sentido como ocurre en otros formularios de certificaciones.

CHAIR DRYDEN: Vamos a tener que pasar a nuestro orador final. Espero que este intercambio pueda continuar offline y vamos a poder hablar de esto también con ustedes en el futuro con el GAC.

Ahora tiene la palabra el Reino Unido y luego vamos a cerrar la sesión.

Reino Unido: ¡Gracias presidente! ¡Y gracias por la presentación!

Nos resulta muy útil y complementa la información que recibimos en Europa de parte de los gobiernos europeos. También lo que nos dijo Luis PIPE NCC en este sentido. Y nos recuerda que el enrutamiento seguro sigue siendo nuestro objetivo para la comunidad. Esperamos que esa meta pueda ser lograda y según recuerdo de los informes europeos que recibimos, era aparente que no toda la industria estaba en línea con algunas de las respuestas que ustedes dieron aquí. Estoy hablando de los ISPs por supuesto.

Para nosotros en los gobiernos, bueno es como que tenemos que seguir viendo que la industria nos está hablando con una sola voz y cuando se trata de ver qué es lo que podemos hacer

para promover la concientización, es como que tenemos una mano atada y de industria buena , decimos hay que encontrar una forma de ir para adelante y allí aparece RIPE NCC y nos muestra el trabajo que hace en esa área y cuáles son los informes.

Seguramente vamos a tener más información en Ámsterdam cuando nos reunamos los gobiernos y espero que podamos tener otros RIR que también nos dé información.

En el ministerio donde yo lidero la asesoría técnica, los puntos técnicos, quiero hacer un par de preguntas básicas no técnicas. Primero si la expansión de Nombre De Dominio que tiene miles de GTLDs posibles para los próximos 10 años y que va a permitir agregar más urgencia a estos trabajos, esa es la primera pregunta. Y la segunda es ¿por qué la implementación del RPKI no va a tener un impacto significativo en el abuso del sistema de DNS? ¡Gracias!

GEOFF HUSTON: la pregunta es simple, la respuesta no. Los nombres y los números funcionan en forma separada en este caso y la expansión del espacio de nombres en la estructura de los nuevos GTLDs no tiene ninguna vinculación con estos recursos de RPKI, son totalmente separados y no tienen relación alguna.

El tema del escalamiento de la inseguridad en el internet, es un tema interesante ciertamente. Hace 15 o 20 años la inseguridad era el producto de un chico de 16 años muy aventurado que no

tenía nada que hacer en la tarde y cuando vemos ahora la inseguridad, esto se ha convertido a una industria, a una industria criminal pero a una industria al fin.

Y ciertamente con el valor de las transacciones en el internet, subvertir la operación normal de internet, es algo que le resulta de interés a los jugadores que no juegan legítimamente y que no merecen nuestra confianza.

Atacar en enrutamiento, es algo que se puede hacer con recursos y con conocimiento y que puede ser un ataque muy efectivo. Se puede atacar a puntos específicos en la red o se puede ampliar el efecto de un ataque. Esta no es una situación cómoda y ciertamente hay medidas para asegurar el enrutamiento que no es que no se hacen porque no tenemos nada que hacer el miércoles que viene, es simplemente porque tenemos una agenda que nos presiona mucho hacer la seguridad.

La infraestructura en la seguridad es lo peor de los problemas que podamos tener. Todo el resto puede funcionar bien, pero si el triangulo va hacia la dirección incorrecta, el triangulo funciona de todos modos, avanza de todos modos. Ciertamente vemos la implementación como un factor de mitigación de las cuestiones potenciales sobre las cuales puede ser subvertida a internet, es decir cuál es el efecto de la base criminal u otras formas de criminalidad que no merezca nuestra confianza.

Entonces sí es importante ¡Gracias!

CHAIR DRYDEN: Les agradezco como siempre a la ASO, a la NRO por haber presentado este tema.

Hubo un alto nivel de interés y por eso no quería evitar que continúe el debate. ¡Espero que podamos volver a este tema en el futuro! y nuevamente les agradezco.

Para el GAC, no nos beneficiamos cuando tenemos almuerzos muy cortos, por eso voy a sugerir el horario de las 2:45 para volver y luego vamos a continuar con nuestra agenda, ¡Muchas gracias! 2:45, 14:45 ¡Que tengan buen almuerzo todos!