MARRAKECH – Sesiones vespertinas de becarios
Miércoles, 9 de marzo de 2016 – 18:00 a 19:30 WET
ICANN55 | Marrakech, Marruecos

VOZ MASCULINA SIN IDENTIFICAR: Sesiones vespertinas de becas, [técnico Alex] [inaudible].

VOZ FEMENINA SIN IDENTIFICAR: Buenas tardes a todos. ¡Vaya! Eso es extraordinario. Miren eso. ¿Están todos despiertos? Cualquiera que esté durmiendo, no es momento ahora. Así que tenemos una tarde un tanto extraña porque los autobuses hacia la gala comienzan a salir a las 19:00. Por lo tanto, queremos intentar aprovechar al máximo el tiempo de nuestros oradores. La reunión anterior a la nuestra finalizó un poco tarde y por más fuerte que intentamos hablar afuera, simplemente no entendieron el mensaje. ¿Qué vamos a hacer? En todo caso, nos excedimos un poco del tiempo esta mañana, así que ese fue nuestro castigo.

Gracias a todos por estar aquí. Espero que todos ustedes hayan tenido un buen día. Mañana por la mañana, tendremos una oportunidad más extensa para entrar y hablar de la semana que hemos tenido. Por lo general, tratamos de utilizar estas sesiones de la tarde para hacer eso, pero hemos tenido tantos oradores que han venido en la tarde que no hemos tenido esa

oportunidad, así que quería hacerles saber que vamos a tener esa oportunidad mañana.

En cuanto a nuestros oradores de esta tarde, Steve Conte y John Crain integran el personal de la ICANN. Son dos de mis colegas y están aquí para hablar con nosotros. ¿Están aquí para hablar con nosotros sobre qué temas, caballeros?

STEVE CONTE: No lo sé aún.

VOZ FEMENINA SIN IDENTIFICAR: Bien. Les he dicho que tenían que prepararse para terminar por lo menos diez minutos antes, así que adelante.

STEVE CONTE: ¿Cuánto tiempo tenemos?, porque sé que pueden hacer una [descarga] también, ¿verdad?

VOZ FEMENINA SIN IDENTIFICAR: Sí, quiero intentar dejarlos ir probablemente unos cinco o diez minutos antes de las 19:00 para que tengan tiempo. Hay otros servicios de transporte, por cierto. No es el único servicio de transporte. Es tan sólo el primer servicio de transporte que sale a las 19:00, así que quiero permitirles salir de aquí antes de

las 19:00. Son cerca de 18:20, así que queremos dejar tiempo suficiente para preguntas.

JOHN CRAIN: De acuerdo, bueno, normalmente suelo decir que estamos entre ustedes y la cerveza, pero he oído que en la gala no servirán alcohol, así que estamos entre ustedes y el agua que igual es algo bueno porque estoy seguro de que la comida será fabulosa. ¿Cuántos de ustedes son becarios por primera vez? ¿Cuántos de ustedes me han visto hablar antes? Muy bien, así que no voy a poner los conjuntos de diapositivas.

Soy el Director Ejecutivo de SSR, Seguridad, Estabilidad y Flexibilidad en la ICANN. Tengo un pequeño grupo a mi cargo, del cual Steve es uno de los miembros. Nos ocupamos de la seguridad de los sistemas de identificación, el sistema de nombres de dominio, el enrutamiento, etc.

Estamos cortos de tiempo, así que voy a pasar directamente a las preguntas. ¿Quién tiene preguntas acerca de Internet o la seguridad, estabilidad o flexibilidad de los identificadores, o tal vez algunas de las cosas que hacemos como los programas de capacitación? Somos el grupo que realiza una gran cantidad de programas de capacitación, y también somos parte del grupo que realiza una gran cantidad de trabajo de investigación. Podemos sentarnos aquí y mostrar los conjuntos de

diapositivas, pero ¿alguien tiene alguna pregunta para nosotros? Voy a comenzar con la joven por aquí. ¿Desea utilizar este micrófono?

VOZ FEMENINA SIN IDENTIFICAR: [Inaudible] [Tajani]. ¿Podría empezar por decirnos de cuáles aspectos de la seguridad se están ocupando en el IPv4 y el IPv6, tal vez? ¿Como el identificador, o como los recursos?

JOHN CRAIN: Bien, en cuanto al IPv6, en realidad no estamos haciendo mucho en este momento. Algunos de los problemas que tuvimos en el pasado estaban relacionados con asegurarnos de que se pueda desplegar el IPv6. Así que cuando consideramos el lado de la ICANN, tiene que ver con cosas como si deseo utilizar el IPv6 en el DNS, por ejemplo, porque DNS se trata de traducir nombres, ¿se puede realmente hacer eso? Si soy un usuario final, ¿puedo en realidad poner mis quad-A, mis direcciones IP en el DNS? Si observan alrededor en los registradores, en su mayor parte ahora se puede.

Así que estas son dos de las cosas que hemos considerado. Hemos considerado cosas como si ponemos colocar quad-A en la zona raíz... esto fue hace unos años y, por supuesto, lo hemos hecho... ¿cuál es el efecto? ¿Qué romperemos al cambiar el

tamaño de la zona raíz, que es un archivo de DNS para los TLD para Internet? ¿Qué romperíamos? Examinamos cosas como esas. Examinamos cosas y decimos: "Bueno, ¿cómo esto va a cambiar las cosas?"

Si observan el Protocolo de Internet Versión 4, la versión 6 tiene algo en común. Hay dos problemas interesantes en este momento. Uno de ellos es el hecho de que no se puede autenticar quién es dueño de qué bloque de IP. ¿Quién juega aquí con los enrutadores? Los envidio mucho. Me quitaron todas mis contraseñas de activación hace años. Ya no me permiten acercarme a los enrutadores.

Pueden asegurar entre dos puristas, dos personas hablando. Pueden utilizar MD5 o algún otro algoritmo para autenticar quiénes son ustedes. No se puede hacer eso a nivel mundial. Hubo varios intentos de arreglar eso. Asegurar el BGP es uno de ellos. El BGP es el protocolo de enrutamiento, una versión segura, y algo llamado RPKI, Infraestructura de Clave Pública de Enrutamiento. Ninguno de ellos se ha desplegado realmente tan lejos. Así que estos son los tipos de problemas de seguridad que consideramos allí.

El otro es que hay algo, lo llaman el mercado gris, el mercado emergente, el mercado del Protocolo de Internet Versión 4.

Podrían no pensar que sea un problema de seguridad. ¿Por qué es un problema de seguridad el hecho de que las personas están comprando y vendiendo direcciones IP? No lo es, pero podría ser un problema de estabilidad. ¿Qué ocurre si, dentro de cinco años o dos años a partir de ahora, las direcciones se vuelven tan caras y tan limitadas que ninguno de ustedes puede obtenerlas? En cierto modo, eso significa que ni siquiera pueden hacer la traducción que hacemos entre v4 y v6. No estoy diciendo que vaya a ocurrir, pero eso es algo que tenemos que considerar y la gente lo está empezando a estudiar.

Yo diría que hace unos cinco o seis años aproximadamente, tuvimos un taller que organizó Google que analizó si habría o no un mercado emergente. Nosotros predijimos que habría y estábamos analizando para ver si le podíamos poner controles. Con algunos de los mejores economistas del mundo y algunas personas de ingeniería excelentes, no pudimos resolverlo. Así que estos son los tipos de cosas que analizamos en el espacio de direcciones.

Obviamente, el agotamiento de los recursos del IPv4 es algo que hemos estado considerando durante años y tratando de lograr que la gente entienda que realmente iba a suceder. Lamentablemente, la gente nunca cree cuando uno les dice que el cielo se está cayendo hasta que le golpee la cabeza.

Hemos estado diciendo: "el IPv4 se está acabando. El IPv4 se va a acabar. No, en serio, se va a acabar muy pronto, pronto".

Todos dicen: "Sí, sí, lo que sea", y entonces un día, la IANA, el bloque de la ICANN, se agota.

Nosotros intentamos predecir estas cosas, a pesar de que la gente no quiera escuchar. Realmente estamos analizando ese lado del asunto más que entrar en las minucias de los detalles de seguridad.

VOZ FEMENINA SIN IDENTIFICAR: [inaudible]

JOHN CRAIN: Sí.

VOZ FEMENINA SIN IDENTIFICAR: En primer lugar, creo que los RIR también están analizando las cuestiones de RPKI e IPv6.

JOHN CRAIN: Absolutamente.

VOZ FEMENINA SIN IDENTIFICAR: Entonces, ¿dónde está la frontera entre lo que la ICANN está haciendo y lo que los RIR están haciendo? En segundo lugar, al principio, pensé que su grupo está trabajando a nivel de infraestructura, pero ahora parecen ser operaciones de principio a fin. ¿Es correcto eso?

JOHN CRAIN: Estamos analizando protocolos también. Estamos analizando las cosas que utilizan identificadores. Lo central es el sistema de identificadores. Esos son nombres y direcciones, números de puerto, todos los sistemas de identificadores. Y sí, los RIR están, por supuesto, analizando todas las cosas en torno a las direcciones IP y también, por supuesto, los números del sistema autónomo. Así que trabajamos juntos.

Yo solía trabajar en el RIPE NCC. Tienen algo allí denominado laboratorios de RIPE, que es un centro de investigación dentro de uno de los RIR, y trabajamos de forma muy estrecha con ellos. De hecho, ¿quién ha oído del programa ATLAS? Somos uno de los patrocinadores de dicho programa. Daniel Karrenberg, la persona que lo diseñó, es uno de mis mejores amigos, así que trabajamos en este tipo de cosas juntos.

Entonces, ¿hay un límite? Sin duda, cuando ustedes entran en el ámbito de la política, pero cuando se meten en realidad a

trabajar en problemas reales, tenemos la tendencia a trabajar mucho juntos.

OSAMA TAMIMI: Buena noches. Soy un becario de la ICANN de Pakistán. Me acaba de surgir una inquietud en términos generales. ¿Están ustedes ocupándose de la seguridad desde una perspectiva de la ICANN y por lo tanto se están centrando en la seguridad del DNS únicamente o están tratando de abarcar un alcance mucho mayor para tener la seguridad de extremo a extremo para Internet?

JOHN CRAIN: No, nos centramos en la seguridad de los identificadores, no sólo del DNS. No estamos considerando una seguridad de extremo a extremo. Eso no nos corresponde. No estamos creando productos de seguridad. No estamos analizando profundamente la infraestructura de otras personas. No podemos. Ese no es nuestro rol. Nuestro rol, según lo dispuesto por los estatutos desde el día en que se fundó nuestra organización, es preocuparnos por la seguridad y la estabilidad, y hemos agregado la flexibilidad porque eso es necesario que cuando las cosas realmente se rompen, de los sistemas de identificadores de los cuales el DNS es uno de ellos. Es muy importante, pero es tan sólo uno.

HAMZA MEHREZ: Hamza Mehrez de Túnez. Tengo una pregunta que puede estar relacionada con la seguridad de los usuarios finales en línea. Mi primera pregunta es: ¿creen ustedes que los usuarios finales deberían utilizar Internet de forma anónima? Y la segunda pregunta es: ¿cuáles son sus recomendaciones frente a las amenazas al desarrollo de la Internet de las cosas?

JOHN CRAIN: Bien, entonces son dos preguntas distintas. Deben ser capaces de tener privacidad. Y el anonimato, palabra que nunca puedo decir porque es tan horrible... anémona, que es la de los dibujos animados con los peces... eso es otro tema diferente. Así que desde un lado de mí, digo: "sí, ustedes deberían poder permanecer en el anonimato". Pero el otro lado de mí dice: "bueno, si me estás atacando, eres un criminal o lo que seas, no quiero que puedas permanecer en el anonimato". Quiero hacer cumplir la ley a través del debido proceso para tener alguna manera de ir y encontrarte. Recuerden que la parte del debido proceso es muy importante.

Yo mismo estoy en conflicto con esto porque hay veces que quiero ser absolutamente anónimo. Cuando entro a Facebook desde el trabajo, no quiero que mi jefe se entere que soy yo navegando por Facebook todo el día, pero también entiendo el

otro lado de la discusión. Así que no es una pregunta sencilla. Si fuera una pregunta sencilla, no estaríamos teniendo todas estas peleas, etc.

Y, ¿cuál era la segunda parte de su pregunta?

STEVE CONTE: La Internet de las cosas.

JOHN CRAIN: Ah, la Internet de las cosas. Tengo una preocupación acerca de la Internet de las cosas, y es que todas son muy baratas. Los dispositivos son baratos. No son tan seguros como deberían ser. La Internet de las cosas es un término de marketing para poner todos sus dispositivos a través de Internet, al igual que la seguridad informática es un término de marketing. Hay una cantidad de términos de marketing que circulan por ahí, la Nube. Son todos términos de marketing.

Así que, ¿estoy preocupado? Juego con dispositivos en casa todo el tiempo. Mis interruptores de luz, que puedo controlar desde el teléfono. Tengo cámaras que también puedo controlar. No se puede hacer nada de esto fuera de mi casa. No puedo hacerlo desde aquí porque estoy preocupado por los aspectos de seguridad, pero dentro de una red controlada, juego con estas cosas todo el tiempo.

Francamente, la mayoría de ellas no están muy bien construidas, pero es tecnología nueva. Los automóviles no estaban muy bien construidos cuando salieron por primera vez, así que un montón de estas cosas, son pequeñas, son más baratas. Las cosas van a mejorar, espero.

STEVE CONTE: [Inaudible] para eso también, si pudiera. Está todo bien. Tengo un micrófono. La primera pregunta que usted tenía. Sí, trabajamos en la ICANN y tenemos un enfoque muy estrecho y específico en lo que observamos en términos de seguridad, estabilidad y flexibilidad. El usuario de extremo a extremo o la conectividad de extremo a extremo no se encuentran realmente dentro de las competencias de la ICANN, pero seamos honestos. Todos somos usuarios finales, así que todos tenemos nuestras propias preocupaciones personales y tratamos de equilibrar eso entre mis preocupaciones personales y mis preocupaciones laborales y cosas por el estilo.

Hay cierta superposición en eso, pero John ha dado en el clavo. No es realmente donde está la competencia de la ICANN. Si salimos del ámbito donde debería estar la ICANN, entonces estamos en un territorio que otros expertos están analizando. Colaborar con ellos es una cosa, pero interferir en su territorio es

otra. Así que tratamos de colaborar con esos grupos cuando resulta pertinente hacerlo.

En el caso de la Internet de las cosas, creo que lo que estamos viendo es un período de rápido desarrollo del producto. Con el rápido desarrollo, que es impulsado por la cuota de mercado más de lo que se trata de estabilidad y la conectividad y la seguridad y todo eso también. Todos están tan pendientes y emocionados acerca de esta Internet de las cosas. Están ignorando una gran cantidad del proceso, aunque viejo y aunque lento, de desarrollo del protocolo adecuado a través de la ITF, que tiene comprobaciones de seguridad para el desarrollo de protocolos. Las personas tan sólo quieren sacar este tipo de cosas.

A veces es genial. Hay algunos servicios buenos por ahí y algunas cosas buenas de Internet de las cosas, pero llevar a cabo el proceso y comprender que si se dejan de lado algunas de esas cosas, se van a generar algunos problemas. Cuanto más y más cosas obtengamos en la Internet de las cosas, eso se va a empezar a agravar.

Estamos empezando a considerarlo desde algunos aspectos. Rick está realizando algunos de los trabajos en materia del DNS de algunas de las cosas de IoT. Estamos empezando a examinarlo y a meter los pies en la piscina para ver si hay algo

que esté dentro del enfoque de la ICANN, pero ahora mismo, sólo estamos viéndolo como personas.

JOHN CRAIN: Sí, y si nos fijamos en todos estos dispositivos, muchos de ellos tienen servidores de DNS activados. Todos van a necesitar direcciones IP. ¿Esas van a ser algún tipo de dirección IP privada? ¿Va a ser v6? Hay una gran cantidad de preguntas que nos tocan, pero no es porque sea la Internet de las cosas. Es porque afectan a nuestro mundo.

¿Alguien? ¿Cuál? Usted modera. Está bien, ¿quién estaba primero? Vamos a empezar con ese. Él tiene su micrófono encendido. Adelante. No, este señor.

VOZ MASCULINA SIN IDENTIFICAR: [inaudible]

JOHN CRAIN: Sí, justo al final.

VOZ MASCULINA SIN IDENTIFICAR: Muy bien, gracias. Muchísimas gracias. Tengo esta aclaración sobre dos [inaudible] de ustedes. ¿Dónde queda el control de la seguridad cuando desea compararlo con el control del gobierno? Debido a que el [inaudible]. Estoy más interesado

en eso, también. Pero lo que sucede cuando los gobiernos deciden controlar nuestra seguridad sucede en el dominio. No sé en qué punto lo hacen.

Daré un ejemplo. En algún punto, mi país y [inaudible] es mi nombre de Nigeria, por cierto. En algún punto, no puedo recordar lo que estaba ocurriendo en ese momento, pero [inaudible] periodo de tiempo [inaudible] o 24 alrededor de la misma, no había Internet. Todo, no se puede iniciar sesión en cualquier dominio en absoluto. Los teléfonos estaban bloqueados. No estoy hablando sobre el teléfono de todos modos, sino de Internet, no se puede iniciar sesión allí. No podemos iniciar sesión en la ICANN. No se puede iniciar sesión.

¿En qué punto vemos las garantías? Por cierto, hay un [inaudible]. El [inaudible] es que la misma persona que esté interesada en bloquear la página web puede estar interesada en poner en peligro la seguridad.

JOHN CRAIN: Los gobiernos hacen lo que hacen los gobiernos. Está hablando de Internet y no del sistema de identificadores. Hemos tenido casos en los que los gobiernos han decidido apagar el ancho de banda por lo que sea que hayan hecho para cortar el acceso. Si lo examinamos, decimos: "¿Hay algún efecto sobre nuestro ecosistema?"

El solo hecho de que algo no esté funcionando en el país no significa que no esté funcionando en el resto del mundo. Una gran parte del tiempo, el DNS y todo para todos fuera de ese país, está completamente bien, al menos si han construido sus sistemas correctamente.

Los gobiernos hacen lo que hacen los gobiernos. No tiene nada que ver con nosotros. Esas son cuestiones políticas nacionales.

Hemos tenido casos en los que ese tipo de cosas suceden y la gente dice, "la ICANN apagó a este país", porque la gente de la prensa dice lo que se le antoja. Nada de eso ha sucedido nunca. Nunca hemos tenido presión de los gobiernos para tomar parte en eso. Aunque sospecho que si la tuviéramos, tan sólo diríamos: "Sí, salgan de aquí". Los gobiernos hacen lo que hacen los gobiernos. Ese no es realmente nuestro ámbito.

Lo que resulta interesante es que tenemos una gran cantidad de gobiernos que participan en los procesos de la ICANN y cuando están aquí, a todos les encanta Internet. Bueno, a la mayoría de ellos. Están diciendo: "Esto es muy importante", y luego de vez en cuando, se ve... y es muy de vez en cuando... se ven cosas como esta que sucedan donde cortarán el acceso a Internet, no siempre a propósito, por cierto. He visto un par de veces en que han hecho estas cosas por accidente.

Es un tema interesante, pero en realidad no es algo en lo cual la ICANN se meta. El GAC nunca se mete en este tipo de cosas. Simplemente no es nuestro ámbito.

[BOB]: Gracias. Quería preguntarle sobre la confianza pública, los problemas de la infraestructura pública. ¿Qué futuro ve usted entre el futuro de las autoridades de certificación y el uso de la autenticación basada en DNS de entidades nominadas?

JOHN CRAIN: Está diciendo dónde las DNSSEC avanzan. Es como todo. Se necesitan solicitudes para construir en la parte superior de eso que la gente utilizará. En lo personal, me gustaría en algún momento que las DNSSEC estén en todas partes y que la gente realmente no piense más en eso. Es tan sólo que el DNS sea seguro. Eso podría llevar años.

Lo interesante es que hay cosas que vienen juntas como la DANE, que es un área del IETF, donde están colocando servicios en la parte superior de las DNSSEC si se quiere, la capacidad de tener sus propios certificados y luego autenticarlos de alguna manera. Si la gente comienza a usar ese tipo de cosas, y algunas personas están experimentando con ellas, entonces tener las

DNSSEC puede tener más beneficios que sólo la autenticación de sus respuestas. Eso será interesante, y eso está comenzando.

La persona con la cual necesitan hablar (los puedo presentar) es un caballero llamado Dan York de la ISOC que tiene que ver con la medición de estas cosas. Tenemos un caballero llamado Richard Lamb que también se encarga de todo lo relacionado con la medición de estas cosas, pero la ISOC tiene una gran cantidad de detalles sobre cómo esto está creciendo y son personas que comienzan a utilizar DANE y otras cosas que se pueden poner encima de las DNSSEC.

Si no construimos nada encima de ellas, si no utilizamos la herramienta, entonces simplemente se las arreglará de alguna manera. Ocurre lo mismo con el Protocolo de Internet Versión 6. Si no tienen una razón para usarlo, la gente no lo hace. Se apegan a lo que conocen. La razón era que el cielo se derrumbó y nos quedamos sin la versión 4, pero todas las otras cosas que prometía la versión 6 realmente nunca le interesaron a nadie.

Creo que usted era el siguiente.

MUHAMMAD SHABBIR: Gracias. Estoy interesado si nos puede decir algo acerca de las técnicas y herramientas que [se implicarían] para garantizar la seguridad de los identificadores. ¿Cuáles son las técnicas, si nos

puede explicar sobre eso? Y para que conste en el registro, habla Muhammad Shabbir de Pakistán.

JOHN CRAIN: Las herramientas son muy simples. Obviamente, existe una investigación, que mide lo que está ocurriendo allí afuera, en busca de diferencias. Pero también hay algo llamado inteligencia de amenazas, que es básicamente hablar con la gente, estar en las listas de correo de seguridad, estar en todos los lugares en los que se habla de todas las cuestiones. Estas son cosas básicas. No hay nada importante.

Tenemos algunos laboratorios. Por ejemplo, tenemos un laboratorio en el que estamos examinando cómo cambian los paquetes a medida que pasan a través de middleware, cosas como los routers de sus hogares y firewalls y VPN. Todas esas cosas generan efectos en los paquetes y los identificadores. Nosotros realizamos la investigación. Tenemos un pequeño grupo de investigación.

Luego, lo otro que hacemos es interactuar con la comunidad. Estamos constantemente hablando con la gente en la comunidad de seguridad sobre lo que se está viendo. Si hay una amenaza, ellos saben que nos tienen que llamar. Si examinamos algunas de las grandes botnets que han generado problemas en la red pero que también afectaron el sistema de identificadores,

son una amenaza porque pueden ser utilizadas para generar un ataque distribuido de denegación de servicio en el sistema, y también, a menudo, se registran decenas de miles de nombres en el sistema que están allí sólo para propósitos nefastos, que a nuestro juicio es un problema.

La mayoría de ellos, no los encontramos. Esa no es nuestra área de especialización, pero sí conocemos a las personas que se dedican a esa área y ellos nos conocen. Gran parte de estar encima de las amenazas y prever las cosas que se vienen no se trata de saber todo uno mismo. Se trata de tener los grupos de pares adecuados para que en realidad se pueda aprender de otras personas.

Lo he visto. Usted es el siguiente. De acuerdo, adelante.

HASHIM NOUMAN: Hashim Nouman de Pakistán. ¿Qué están haciendo para detener los CGN?

JOHN CRAIN: Nada. El NAT masivo o Carrier-grade NAT. Nada. Estamos observando con desconcierto.

STEVE CONTE: Y un poco de temblores también.

JOHN CRAIN: Sí, y un poco de temblores. Tanto si utilizan un Carrier-grade NAT o si optan por algo como la Versión 6, la cual sería mi preferencia, es una decisión de negocios. La gente lo está considerando mucho desde una perspectiva comercial.

Ahora bien, si están del lado que desea ver lo que está ocurriendo en la detección de vulnerabilidad, en busca de los malos actores, cosas por el estilo, este [uso de NAT] en las direcciones a gran escala y los problemas asociados con el registro de esto son problemáticos.

Mi preocupación personal sobre los Carrier-grade NAT es que la gente invertirá, siguiendo en este camino, una gran cantidad de dinero (no son baratos) y luego no tendrán, tal vez por muchos años, ningún incentivo para optar por la Versión 6. Si esto viene de forma predeterminada, todos los grandes ISP dicen: "Bueno, Carrier-grade NAT, porque tiene todas estas funciones geniales, es el camino que seguiremos", por cualquier sentido de propósito comercial que hayan decidido esto. Me preocupa el efecto sobre el despliegue de la Versión 6 y llevarla a los extremos, etc. Pero estas son decisiones de negocio así que es muy difícil generar influencia en ellas.

STEVE CONTE: Tan sólo para agregar a esto un poco, también, estoy totalmente de acuerdo con lo que John acaba de decir, pero cuando se hace un CGN y cosas por el estilo e incluso simplemente el NAT, usted o su dispositivo están cambiando lo que el paquete estaba destinado a ser en primera instancia. Así que ya está cambiando su verdadera conectividad de extremo a extremo tan sólo al poner un solo NAT en alguna parte.

Reconozco que tiene cierto beneficio. Tengo toda una red. Tengo NAT y lo uso, pero cuando se pone NAT, en NAT, en NAT, en NAT, entonces se rompe mucho más y mucho más y mucho más. No es un problema de la ICANN, pero es un problema que se debe considerar. Estoy seguro de que hay otras personas por ahí que están examinando si se están rompiendo cosas o no y en qué nivel.

Como John ha dicho, es una decisión comercial. Si un ISP decide utilizar CGN y rompe su base de clientes, es algo horrible para el cliente. Estoy de acuerdo, pero no necesariamente afecta la estabilidad o la flexibilidad de Internet en su conjunto. A menos que por alguna extraña alucinación colectiva decidimos poner el CGN realmente en el núcleo del enrutamiento, entonces sí realmente se convierte en un problema del cliente o en un problema de la empresa cuando las cosas no funcionan. No es una gran respuesta, pero ahí es donde estamos.

JOHN CRAIN: También deben recordar que cada vez que entramos en las áreas que son de color gris para nosotros, recibimos un disparo. Tenemos mucha presión para mantenernos dentro de sus límites. Así que cosas como esas, están justo en esa zona gris. Participamos en los debates porque la gente acude a nosotros por nuestra experiencia, y queremos aprender. Pero no va a ser algo sobre lo que alguna vez la ICANN elaboraría una política o algo por el estilo. No es en ese ámbito.

¿Tenía un comentario al respecto o una pregunta?

VOZ MASCULINA SIN IDENTIFICAR: ¿[Inaudible] CGN?

JOHN CRAIN: ¿Desean hacer eso?

VOZ MASCULINA SIN IDENTIFICAR: ¿Saben lo que es NAT? Si tienen un router en casa y tienen una dirección IP pública, el router convierte eso en varias direcciones IP. Un Carrier-grade NAT o NAT masivo es lo mismo, pero, por extraño que parezca, a gran escala. Está en una empresa de telefonía celular o un cable o ISP, donde, debido al agotamiento de v4, sólo tienen tantas direcciones IP públicas,

pero necesitan servir a 1.000 veces la base de clientes de lo que tienen para las IP públicas. Están convirtiendo eso en un gran NAT en el comienzo de su red.

JOHN CRAIN: Cosas como que mantienen las direcciones por lapsos de tiempo muy cortos. Los tiempos de arrendamiento son realmente cortos y registrar ese gran cambio es extremadamente difícil, dicen.

VOZ MASCULINA SIN IDENTIFICAR: Intensivo en cuanto al tamaño, también.

JOHN CRAIN: Este caballero en la parte posterior, creo.

VOZ MASCULINA SIN IDENTIFICAR: Es la misma persona.

JOHN CRAIN: Ah, se ha movido hacia delante. No se mueva.

[JOHN CHAND]: Hola, John de Fiji. Hablando sobre la seguridad del DNS, ¿cuáles son las amenazas de imagen para el DNS? Primera pregunta. Y la

segunda pregunta es ¿cómo manejan la [ética de los proveedores] en los servidores del DNS?

JOHN CRAIN: Ha respondido a la primera pregunta con la segunda. Uno de los mayores problemas, en mi opinión, es la DDoS. Solíamos tener un montón de problemas con cosas como el envenenamiento de caché. Eso ahora ocurre menos debido a las soluciones. Se examinan estos problemas, se buscan soluciones. [Implicaciones] y todos los demás servidores hicieron aleatorización de puertos para que sea más difícil de adivinar qué puerto se utilizaría.

Disculpen si me estoy poniendo demasiado técnico aquí. Es difícil no hacerlo con estas cosas.

Luego tuvimos las DNSSEC encima de eso y el envenenamiento de caché, las mentiras sobre los nombres del DNS ha quedado más en el fondo. Todavía hay maneras de hacerlo. No es perfecto. A medida que desplegamos las DNSSEC, etc., se está mejorando.

¿Quién de ustedes ha sufrido un ataque de DDoS? Ataque de denegación de servicio, deja inactiva su red. Es realmente deprimente. No hay mucho que puedan hacer al respecto. Ustedes aprovisionan y aprovisionan más, que es caro, y

solicitan a sus ISP que aprovisionen más el canal de subida y se puede hacer un poco de filtrado.

Pero si alguien realmente quiere atacarlos con una DDoS, simplemente van a sufrir el dolor. Han visto organizaciones muy grandes recibir ataques de DDoS que tienen los fondos, corporaciones de miles de millones de dólares que tienen los fondos para adquirir infraestructura e incluso ellos sufren ataques de DDoS.

Antes veíamos una tendencia muy grande en el crecimiento del tamaño de los ataques de DDoS individuales, y todavía estamos viendo algo de eso. No he mirado las estadísticas recientes, pero hemos visto ataques de DDoS en el rango de medio terabyte.

¿Quién de ustedes tiene medio terabyte de ancho de banda en su red? Sí, nadie. Pero ahora lo que estamos observando es que se ven ataques de DDoS cada vez más pequeños. Estamos viendo que se utilizan para diferentes tipos de actividad delictiva. Una gran parte del tiempo, eran algunos de estos grandes que realmente estaban relacionados con expresiones políticas y el tipo de cosas como "No me gustas; Voy a acabar contigo". Pero ahora estamos observando una gran cantidad de chantajes y cosas por el estilo. Estamos observando una gran cantidad de extorsión a través del delito.

Debido a las DDoS, botnets, redes de máquinas comprometidas, en mi opinión, son uno de los grandes problemas de la red y no hemos encontrado una buena solución. Aun cuando sabemos dónde están, que hay maneras en las que podemos hacerlo (examinamos las botnets porque creemos que son una amenaza), incluso si identificamos una máquina que está comprometida y es parte de una botnet, no hay realmente mucho que podamos hacer al respecto. Son una víctima, pero ni siquiera podemos reparar su máquina porque eso sería ilegal.

Los delincuentes pueden salirse con este tipo de cosas porque no les importa, pero no se puede en realidad, en la mayoría de las jurisdicciones, ir y reparar la máquina de alguien sin su consentimiento explícito.

Así que cuando lo hicimos [Configurar] que fue hace años, teníamos las direcciones IP y los millones de máquinas que estaban infectadas, pero todo lo que podíamos hacer era acudir a los ISP y esperar que fueran e hicieran algo. No podíamos hacer nada en realidad a pesar de que técnicamente, probablemente podríamos porque tenemos algunas mentes muy inteligentes en la sala. Ustedes se sientan allí y dicen: "Si tan sólo hiciéramos esto, podríamos hacer que todo desaparezca".

STEVE CONTE: Pero tan sólo recuerden que el propietario de la máquina comprometida no es el malo de la película. Es su madre.

JOHN CRAIN: Tanto a nivel moral y legal, era como, sí, no es hacer lo correcto. Así que esa es probablemente la mayor amenaza, creo, por lejos. De hecho, tenemos un documento que muestra una serie de diversas amenazas para el ecosistema, pero muchas de las amenazas cuando la gente las observa, están en realidad dirigidas hacia el lado comercial de la misma, no necesariamente tecnología propiamente dicha. Pero la DDoS, es por lejos la mayor amenaza en este momento.

VOZ MASCULINA SIN IDENTIFICAR: [inaudible]

JOHN CRAIN: [Inaudible] mirar. Ese es el.

VOZ MASCULINA SIN IDENTIFICAR: Habla [inaudible] de Gambia, becario por segunda vez. Mi pregunta, quisiera plantear nuevamente la cuestión de la Internet de las cosas. Mi pregunta es la siguiente: ¿es realmente necesaria la Internet de las cosas? ¿La necesitamos? Porque

para mí, no veo ninguna [inaudible] para inventar la Internet de las cosas.

STEVE CONTE: ¿Tiene un teléfono móvil?

VOZ MASCULINA SIN IDENTIFICAR: Sí. Bien. Una vez más, mi segunda pregunta es: ¿cuáles son las políticas? ¿Cuáles son las normas o leyes disponibles para poder proteger a las personas con todos los desafíos de seguridad que enfrentamos? Porque hoy en día ni siquiera se necesitan esas destrezas técnicas para ser un hacker porque tienen todas las herramientas disponibles en línea donde se puede ir y descargarlas de forma gratuita. Así que cualquiera puede ser un hacker. ¿Cuáles son las políticas o reglas disponibles para proteger o al menos rescatar a estos programas, este software del fácil acceso?

JOHN CRAIN: Es un mercado abierto. No hay reglas reales. Hay leyes. Hay leyes en todos los países. Si usted ataca a alguien con DDoS para extorsionarlos por dinero, eso es extorsión. Eso es un delito en ese país. El problema es el hecho de que la mayoría de las cosas no están en un país. La víctima puede estar en un país, pero todo cruza jurisdicciones. Hay convenciones como el Convenio

de Budapest y otras convenciones que se ocupan de hacer cumplir la ley en estos casos. Estos no son asuntos de la ICANN. No pertenecemos a la aplicación de la ley. No somos una organización gubernamental. La aplicación de la ley y la protección de la sociedad es realmente una tarea de los gobiernos, y ellos hacen las leyes.

Ahora bien, un montón de leyes viejas, es decir, las leyes físicas, en realidad se pueden utilizar para Internet. El delito es delito en su mayor parte. Hay muy pocos delitos que son realmente delitos de una computadora a otra. Hay muy pocos delitos que son realmente delitos informáticos. Son normalmente delitos contra personas o contra el patrimonio, y existen muchas leyes para hacer frente a eso.

Ahora, resulta muy difícil enseñar a los jueces y abogados y legisladores a pensar de esa manera y entender estas cosas. Internet es algo bastante nuevo. Nos queda un largo camino por recorrer, pero esa no es la tarea de la ICANN. Esa es tarea del gobierno y de las personas que asesoran a los gobiernos.

¿Necesitamos la Internet de las cosas? Bueno, Steve le preguntó si tenía un teléfono. Esa es una cosa. Está conectado a Internet y por lo tanto usted necesita esa pieza de la Internet de las cosas.

STEVE CONTE: Sí, les he pedido que piensen en la Internet de las cosas. Creo que es simplemente una manera de modelar eso. Ellos necesitaban una forma de denominar el hecho de que ahora hay más dispositivos que personas en Internet. Antes, había una computadora en una familia y su familia de cuatro o familia de cinco miembros compartiría esa única computadora, por lo tanto, tenía más personas utilizando Internet que dispositivos. Ahora eso ha cambiado. Creo que si piensan en la Internet de las cosas simplemente como una forma diferente de pensar acerca de cómo y qué hay en Internet y le quitan el aspecto de marketing, entonces eso es realmente lo que es. Es tan sólo un rápido despliegue de más dispositivos que se encuentran en Internet.

JOHN CRAIN: Sí, y se pueden preguntar si desean o no que la luz de su casa se pueda controlar con su teléfono. Ahora, ¿Se necesita eso? Necesitar es palabra mayor. Se necesita comida. Se necesita agua. Se necesita alguna forma de energía probablemente, aunque es probable que se pueda vivir sin ella, así que necesitar es palabra mayor. Claramente existe un mercado. Existen evidentemente buenos usos para la Internet de las cosas.

Así que en mi casa, porque soy un fanático de la informática y juego con estas cosas, si hay un incendio, mis alarmas contra

incendios se activarán. Todos tenemos eso, pero las mías de hecho están conectadas a la red. Así que cuando se activan, ¿qué más ocurre? Todas las luces de mi casa se ponen de color naranja y se encienden porque el color naranja es un espectro de luz que atraviesa el humo. Si detectan humo, también pueden aspirar la casa mediante el uso del sistema de aire acondicionado para sacar el humo.

A veces, las cosas pueden ser más inteligentes y útiles y en realidad tienen propiedades que pueden salvar vidas cuando se pueden comunicar entre sí. Todo sale mal cuando falla la seguridad, pero hay usos muy claros y útiles de dispositivos que al conectarlos, de repente adquieren una utilidad completamente nueva.

Si piensan en un termostato en una casa, ¿cuántos de ustedes suben el termostato y cambiar la temperatura cada vez que piensan que necesita un ajuste? Ustedes dirán: "Ah, sí, lo dejo así. Ya bajará". O puede ir y hacerlo una o dos veces a la semana o una vez al día, dependiendo de qué tanto calor haya. Estará funcionando una cantidad de veces cuando no lo necesita. Eso es desperdiciar energía. Si observan algunos de estos termostatos de aprendizaje que tienen algoritmos que pueden obtener otros nuevos y pueden ser programados a distancia, por ejemplo, mi termostato. Puedo firmar con mi compañía de electricidad, lo cual no he hecho porque no confío en ellos, para

obtener un programa en el que cuando la temperatura sube por encima de un valor determinado, mi temperatura del aire acondicionado subirá. Así que no voy a estar enfriando tanto. Esa es una utilidad real. Si se logra que toda una ciudad de gente lo haga, en realidad estarán marcando una diferencia para el ecosistema.

Necesitar es palabra mayor. Creo que no necesitamos ninguna de estas cosas. No necesitamos Internet. Necesitar. Pero muchachos, sí que está haciendo la vida más fácil. No necesitamos los teléfonos móviles, pero son muy convenientes. No necesitamos termostatos que se conectan a Internet. No he logrado averiguar cuál es la razón para que un refrigerador se conecte a Internet, pero la gente me dice que las hay. O una tostadora. Pero, el mercado impulsará eso.

Creo que muchos de los aparatos desaparecerán con el tiempo, pero creo que algunas cosas resultarán extremadamente útiles.

STEVE CONTE: John, el jefe ha dicho dos preguntas más, pero usted está conversador, así que respondamos una última pregunta y luego déjelos salir a tiempo.

JOHN CRAIN: No estoy conversador. Es que me gusta hablar mucho. Voy a responder dos y las haremos breves. Vamos a seleccionar a este caballero primero y luego seleccionaremos a ese caballero después porque ninguno de ellos ha preguntado.

ANAND RAJE: Anand Raje, becario de la India. Estamos observando una transformación muy grande en el espacio de Internet a medida que avanzamos hacia la Internet de las cosas que el IPv6 [inaudible] está ocurriendo. Así que su comentario experto sobre dónde cree usted que estaremos dentro de diez años con respecto a Internet porque ahora vemos que los sistemas raíz como los sistemas europeos de red abierta de servidores raíz (Open Root Server) [inaudible] DNS que se avecina. Entonces ustedes están teniendo sistemas anónimos que se mantienen al día como la web profunda y la web oscura. Y los problemas de privacidad están ahí. Estamos teniendo automóviles sin conductor, así que las cosas están allí.

Entonces, ¿cómo siente que será eso después de estos diez años?, ¿hacia dónde nos dirigimos?

JOHN CRAIN: Bueno, no puedo ver el futuro, pero puedo hacer un par de comentarios e intentar hacerlos rápidamente para que este

caballero tenga la oportunidad de participar. Estos otros sistemas de DNS alternativos, si pueden encontrar una manera de hacer que todos se comuniquen, sería genial. No creo lo vayan a hacer porque hemos estado diciendo esto durante años. Si todos van por caminos separados, no habrá Internet. Habrá varias Internets y entonces tal vez no podamos hablar uno con otro. Así que tenemos que encontrar una manera, si vamos desde Internet hacia Internets, de cruzar esas fronteras. Porque no estoy diciendo que sea algo malo o algo bueno. Yo personalmente tengo problemas al respecto. Me gusta la idea de que si envío un correo electrónico, que siempre vaya al mismo lugar. Tal vez haya alguna tecnología que pueda resolver eso. La gente está trabajando en eso.

No sabemos dónde estará Internet dentro de diez años. Las nuevas tecnologías vienen. Las nuevas tecnologías se van. Tal vez ni siquiera exista el DNS. ¿Quién de ustedes realmente utiliza, como ser humano, el DNS? Steve y yo, que somos raros. Ustedes tienden a utilizar principalmente cosas como motores de búsqueda y aplicaciones. Tal vez están en el fondo, pero puede ser algo sin importancia para el usuario real, y a esa altura, la gente será menos codiciosa y política al respecto porque no tendrá tanto valor. Eso puede cambiar, pero sólo la tecnología lo impulsará.

Voy a dejar que participe este caballero.

VOZ MASCULINA SIN IDENTIFICAR: [inaudible]

JOHN CRAIN: Voy a dejar que Steve responda la pregunta que sea.

[HAMAD USAMA]: [Hamad Usama] de Marruecos. Bienvenidos a Marruecos. Mi pregunta es acerca de su estrategia de futuro en su nueva estabilidad y flexibilidad y cómo podemos implementarla en el futuro. Sobre la segunda información sobre la Internet de las cosas, organizamos la confianza de lo que la Internet de las cosas en términos de [inaudible]. Fue muy interesante, pero todos los seres humanos no sabemos por qué necesitamos esto. Es para [facilitar] nuestra vida o simplemente para estar con la nueva tecnología. Gracias.

JOHN CRAIN: Se lo dije, usted la responderá.

STEVE CONTE: Así que para responder a la primera pregunta, pregúntele a John. Volviendo al tema de la Internet de las cosas, no creo que sea ya una cuestión de necesidad o deseo. Si nos fijamos en el sistema telefónico lo largo de los últimos 100 años, 120 años que

ha estado entre nosotros, es muy parecido al mismo modelo de Internet en el que sólo lo tenía si usted lo tenía. Luego, más gente lo tuvo y de repente todo el mundo tenía que tenerlo, y ahora usted lo lleva en el bolsillo. Eso que lleva en el bolsillo es la parte de la Internet de las cosas. Así que ahora tenemos Internet y la hemos tenido durante 25 años. Luego más personas la consiguieron y luego las empresas decidieron vender cosas allí. Ahora estamos en el punto en el que todo habla en Internet. Ya no se trata necesariamente de una cuestión de si necesitamos o deseamos cosas. Es como lo que dijo John. Su sistema le habla a otros dispositivos y eso, por lo tanto, hace que su vida sea mejor o más segura o cosas por el estilo.

Ellos siempre van a lanzar todo un refrigerador con televisión incorporada y que llamará automáticamente al almacén por usted, y eso no es la Internet de las cosas. La Internet de las cosas son estos diminutos, pequeños sensores, que están trabajando en conjunto para hacer que alguien o la vida de alguien sea mejor y más práctica. Creo que va a suceder de forma natural. No necesariamente tiene que tener un apodo o una etiqueta de la Internet de las cosas. La humanidad se esfuerza mucho por no trabajar. Eso es lo que estamos haciendo. Estamos trabajando arduamente para que no tengamos que trabajar.

JOHN CRAIN: Primera pregunta, estrategia. Cuando hablamos de estrategia de SSR, estamos a punto de publicar un nuevo documento.

STEVE CONTE: ¿Estrategia de SSR? ¿El marco?

JOHN CRAIN: Sí, el marco.

STEVE CONTE: Nuestro marco, tenemos un nuevo marco para la SSR. Se va a publicar en nuestro sitio web, probablemente en el próximo mes.

JOHN CRAIN: Tenemos que publicar la forma en que estamos pensando estratégicamente para los próximos años, y lo hacemos casi todos los años. Examinamos lo que creemos que son las amenazas emergentes, donde creemos que tenemos que poner nuestras cosas, así que tienen que planificar a futuro.

STEVE CONTE: Y entonces le solicitamos a la comunidad que lo revise. Es un proceso doble. Decimos: "Esto es lo que pensamos que vamos a

hacer", y luego se lo llevamos a la comunidad. Vamos a tener una escena de revisión de la comunidad. Pregúntenme sobre revisiones. Durante el período del próximo año y medio, vamos a estar llevando a cabo conversaciones con el comité seleccionado de la comunidad para determinar si es o no a) lo que estamos haciendo lo que dijimos que íbamos a hacer, pero b) lo que decíamos que íbamos a hacer en nuestra estrategia de futuro es lo correcto que hay que hacer.

JOHN CRAIN: A la gala o no.

VOZ FEMENINA SIN IDENTIFICAR: Muchísimas gracias. Al igual que con todas las cosas, me gusta ofrecer el tiempo de todos así que si ven cualquiera de estos muchachos, por favor deténganlos y háganles preguntas.

JOHN CRAIN: Busquen personas con sombreros raros. Por lo general, somos nosotros.

VOZ FEMENINA SIN IDENTIFICAR: Así que muchas gracias por venir y todos a la gala y a disfrutar de la noche. Los veré muy temprano mañana por la mañana y puntuales.

STEVE CONTE: Antes de que todos se pongan de pie, una última declaración. No tiene nada que ver con seguridad y estabilidad. Tiene todo que ver con ustedes. Ustedes son realmente la voz de la Internet, y el hecho de que ustedes quieran estar aquí y que no se les pague por estar aquí dice muchísimo. Así que sigan así y sean lo que quieran ser y hagan que Internet sea lo que ustedes quieren que sea porque es de ustedes, es nuestra. Aplaudo a cada uno de ustedes por estar aquí. Gracias.

[FIN DE LA TRANSCRIPCIÓN]