ICANN68 | Foro virtual de política – Sesión plenaria: El DNS y el internet de las cosas: oportunidades, retos y desafíos
Martes, 23 de junio de 2020 – 13:00 a 14:30 MYT

RIA OTANES: Hola, y bienvenidos a la sesión plenaria de DNS y el internet de las cosas: Oportunidades, retos y desafíos. Soy Ria Otanes y soy la gerente de participación remota para esta sesión.

Tengan en cuenta que esta sesión está siendo grabada y que sigue los estándares esperados de conducta de ICANN. Durante esta sesión se van a permitir comentarios y preguntas que se presenten en inglés en las preguntas y respuestas en la barra de Zoom. Voy a leer las preguntas y los comentarios en esta sesión. Si quieren hacer una pregunta o hacer un comentario verbalmente, levanten la mano.

Les vamos a dar permiso para que habiliten sus micrófonos y así van a poder tomar la palabra. Digan su nombre y en qué idioma quieren hablar si es que van a hablar en otro idioma que no sea inglés. Esta sesión incluye transcripción e interpretación. Para poder ver la transcripción en tiempo real hagan clic en el botón de closed caption en la barra de Zoom.

Para asistir a nuestros intérpretes, por favor hablen a una velocidad razonable. Para escuchar la interpretación van a tener que descargar la aplicación de interpretación, pueden encontrar más información en la

sesión de detalles y las instrucciones en el chat. Por último, quiero recordarles que utilicen el menú en el chat para cambiar de responder a todos los panelistas hacia responder a los panelistas y asistentes, si quieren que todos en la sala lean sus comentarios.

Con esto, ahora le doy la palabra a Alejandra Reynoso. Alejandra, adelante, por favor.

ALEJANDRA REYNOSO: Muchas gracias, Ria. Bienvenidos a todos. Me llamo Alejandra Reynoso y trabajo para el ccTLD de Guatemala que es el .GT y soy quien va a presidir esta plenaria.

El internet de las cosas quiere hacer nuestra vida más fácil y nuestras sociedades más sostenibles a través de miles de millones de dispositivos conectados que funcionan en nuestro entorno físico. Eso hace que IoT sea diferente de las aplicaciones de internet, como el email y los navegadores, y muchos dispositivos IoT van a utilizar el Sistema de Nombres de Dominio para ubicar los servidores remotos.

El Comité Asesor de Seguridad y Estabilidad, el SSAC, recientemente publicó el documento SAC105; un informe que discute las oportunidades y desafíos de la interacción entre el DNS y la IoT. En el plenario de hoy vamos a darle más sustancia al diálogo que se documenta, específicamente permitiendo que los miembros de la comunidad de todas las Unidades Constitutivas puedan discutir los temas con unos expertos y con otros.

Esta sesión plenaria es un seguimiento a la sesión del SAC105 de la reunión de Montreal que tuvo como foco en particular los ccTLDs. Las metas de estos plenarios son: Entender mejor cómo el internet de las cosas es diferente de las aplicaciones interactivas tradicionales de internet y cómo utiliza el DNS. Para poder entender mejor cómo funciona la interacción entre los jugadores de los distintos ecosistemas en términos de oportunidades, riesgos y retos, y también pensar en el rol que la comunidad de la ICANN puede tener en este espacio.

Siguiente diapositiva, por favor. Esta va a ser la agenda de hoy; primero va a haber una revisión general del documento SAC105; luego vamos a hablar con un panel de expertos para compartir sus perspectivas; después va a haber una revisión de pares donde los revisores van a dar feedback sobre las presentaciones de los expertos; y vamos a terminar con preguntas y respuestas de la audiencia. Siguiente diapositiva.

Brevemente, quiero introducirles a Cristian Hesselman, quien les va a dar un contexto del SAC105. Cristian es el director de SIDN Labs que es el equipo de investigación de SIDN, el operador de .NL de los Países Bajos. Su meta es mejorar la seguridad y estabilidad de las comunicaciones en internet de punto a punto a través de mediciones empíricas y de la realización de prototipos y de herramientas.

Cristian también es miembro del SSAC y del grupo de trabajo que produjo el SAC105 sobre DNS riesgos y desafíos. Y también es profesor asociado en una universidad en los Países Bajos y es parte del Directorio de NLNetLabs. Cristian, tiene la palabra.

CRISTIAN HESSELMAN: Muchas gracias. Es un honor hoy darles una perspectiva general del SAC105 que es el informe que el SSAC publicó en junio. Y como ya se ha dicho, este documento está entre el internet de las cosas y el DNS con un foco en particular de facilitar la discusión en la comunidad de la ICANN.

Este informe también va a aparecer en una revista que se llama IEEE Internet Computing. Siguiente diapositiva.

El internet de las cosas. Lo que nosotros usamos como definición en nuestro informe es la definición que el ISOC dio en el año 2015, que es una aplicación que extiende la conectividad de la red a objetos, dispositivos, sensores y cuestiones que no se consideran normalmente computadoras.

Es decir, conectar todo a la red de un modo diferente de como lo conectábamos antes. Las diferencias con las aplicaciones tradicionales, como el email o un navegador, son las siguientes: La IoT continúa censando e interpretando lo que está en el espacio físico y también interpreta la información que recibe de distintos sensores para actuar en ese espacio.

Esto suele ocurrir sin que el usuario se dé cuenta, es decir, que son cuestiones que están embebidas en paredes o en otros objetos, y que interactúan sin que lo sepamos. Esto es lo que ISOC considera interacción pasiva, y no interacción interactiva que es lo que ocurre con el email y los navegadores, por ejemplo.

Va a haber una gran cantidad de estos dispositivos IoT, al menos esa es la proyección de muchos analistas del mercado. La gente está mencionando números de veinte mil millones a treinta mil millones que básicamente están operando en nuestra vida, no los vemos y que interactúan sin que lo sepamos.

También una diferencia es que los dispositivos IoT son mucho más heterogéneos de lo que nosotros estamos acostumbrados, como las laptops y los teléfonos, tienen distintos tipos de sistemas operativos. Estamos hablando de una arquitectura de hardware diferente, y también estamos hablando de distintos tipos de redes, es decir, que no es solamente Wi-Fi, sino ZigBee y otros tipos de redes inalámbricas.

Y finalmente, IoT también es diferente en el sentido de que tienen una vida mucho más larga, los dispositivos IoT están en estructuras físicas, y por eso son caracterizados como una operación no asistida, es decir, que no hay un gerente de red. Los dispositivos simplemente están allí y se conectan a la red sin que nosotros lo sepamos.

IoT se considera importante porque va a haber en el futuro próximo. Desde los años 90 ya existe la computación invasiva, es decir, que se le ha dado distintos nombres a más o menos el mismo concepto y ahora, estamos llegando a una etapa donde es posible implementar efectivamente estos dispositivos y estos actuadores.

Y como resultado la gente considera, o al menos se tiene una creencia muy establecida, de que IoT va a generar una sociedad más establecida en el área de sistemas de trasportes inteligentes, re-ruteo de sistemas

de trasporte con distintos tipos de sensores o redes de energía inteligente o quizás hogares inteligentes y ciudades inteligentes.

Estos son los ejemplos que todos conocemos por todo lo que vemos o por todos los dispositivos que tenemos en nuestras casas hoy en día. Hay una gran promesa, pero hay un tema muy importante que es el de la seguridad de la IoT. Este es un ejemplo de un modelo que utilizamos en SSAC. Estamos pensando en el internet de las cosas y entonces lo que vemos aquí es una imagen de los espacios físicos a la izquierda. Vamos a tomar la parte superior.

La parte superior izquierda. Eso es lo que ve la gente en sus casas y así interactúa con lo que llamamos implementación de IoT, es decir, lo que está en gris y que ustedes ven en la mitad de la pantalla, y las implementaciones de IoT consisten en tres cosas; uno, son dispositivos de IoT; dos, conectividad de red; y tres, servicios back-end.

Como ejemplo, vemos un reloj inteligente donde la gente se acerca a la puerta de su casa, y quizás tiene una manija de la puerta que también es inteligente, un timbre que es inteligente y todo lo maneja desde el reloj en combinación con huellas, y toda esa información se envía a internet a un servidor remoto y en base a ese servicio se toma una decisión como, abrir la puerta o no. Esto, por supuesto, tiene políticas de usuarios.

Lo que estamos viendo entonces es que en este ejemplo muy sencillo hay información que envía un dispositivo, como un reloj inteligente y esa información se comparte en internet a través de un servicio, y luego,

se vuelve a enviar a la puerta para que la cierre o no. Entonces se "sensea" y se actúa en relación con este entorno físico del usuario, y esto ocurre sin que los usuarios se den cuenta.

Es decir, que los usuarios solamente ven los dispositivos, ven su reloj inteligente o su manija de la puerta inteligente, pero no ven a una persona sentada en una oficina. Y una parte importante de la maquinaria de todo esto es el DNS, porque lo que sabemos a partir de la investigación previa, es que estos dispositivos interactúan con servicios que están en internet para poder brindar sus funciones.

Esto es diferente de los navegadores tradicionales donde uno interactúa con ese navegador para tomar información, para usar un servicio, por ejemplo, y en esta constelación los dispositivos usan servicios para cumplir su función. Por ejemplo, se especifica que un servicio puede tener información central y se toma la decisión de abrir la puerta o no.

En estas interacciones con el DNS, el DNS tiene un rol muy importante, no voy a hablar de los detalles porque ya alguien va a hablar de eso más adelante, después de esta presentación. Creo que esta es la parte más importante por ahora. Continuamos ahora sí con la siguiente diapositiva, por favor.

Muy bien. Este informe se llama DNS riesgos y retos del IoT. Vamos a hablar primero de los riesgos, y después de los desafíos. Las oportunidades son cosas de las que no hablamos mucho con el DNS porque, en general, nos focalizamos en los riesgos como deberíamos

hacerlo; pero en este caso nos pareció que podría haber una oportunidad para el DNS, porque se trata de una infraestructura global de confianza que podemos aumentar la seguridad y la transparencia del internet de las cosas a través de ellos. El DNS puede agregar un valor en este sentido.

Vamos a encontrar un poco más de detalles en el SAC105. Lo primero, es que pensamos que el DNS puede reducir el riesgo de que a los usuarios se les genere un perfil, y esto es porque estos dispositivos interactúan con el DNS. Las consultas entonces de DNS si hay un observador entre la ruta del dispositivo IoT y el servicio remoto que utiliza, puede ver que en base a las interacciones de DNS qué es lo que una persona, por ejemplo, en su casa, qué tipo de dispositivo está usando o incluso si está usando un dispositivo porque eso crea más interacciones con el DNS.

Otra posibilidad es que si uno sabe cuál dispositivo de IoT se está utilizando, al mirar el nombre de dominio, se puede incluso como atacante tratar de ver cuál es el dispositivo de IoT que está generando estas consultas, es decir, que hay algunas investigaciones que muestran que muchos dispositivos utilizan los nombres de dominios que consultan para encontrar ese servidor remoto, como vimos en la diapositiva anterior.

Y muchas veces estas consultas al DNS o los nombres de dominios revelen información sobre el tipo de dispositivo que los está generando, es decir, que el pensamiento por detrás de todo esto es el de generación

de perfiles y se puede encriptar el pedido del DNS, se puede hacer, por ejemplo, a través de DoH y DoT que tienen mucho debate.

Otra oportunidad que nosotros vemos, es que para mitigar un riesgo con un dispositivo IoT se le puede reenviar a otro servidor remoto, por ejemplo. Estamos viendo en internet un concepto que se llama route hijacks, y esto resulta en que el tráfico se reenvía a una red maliciosa. Esto es algo que podría tener unos efectos muy severos en IoT porque los dispositivos IoT no se conectan ya más con el servicio del cual se deberían conectar, y quizás se conectan a un servicio malicioso.

Y el riesgo aquí es que estemos compartiendo los datos íntimos quizás, con servicios remotos o que esos servicios remotos puedan interactuar en un entorno físico. Nos parece que el DNS puede ayudar aquí porque obviamente tenemos DNSSEC que puede validar la integridad de los mensajes que surgen a partir del DNS, y si ocurre este secuestro, por ejemplo, el cliente de DNSSEC va a poder detectarlo porque va a darse cuenta que no se valida la firma en los mensajes de DNSSEC.

Otra oportunidad que vemos es que puede ser una oportunidad para que los registradores puedan dar autenticación multifactor, y pueden así proteger los nombres de dominio que está siendo utilizado por los dispositivos IoT al tener múltiples factores, por ejemplo, reconocimiento de huellas dactilares. Y estas son las dos oportunidades que vemos para reducir el riesgo de que los dispositivos IoT sean redirigidos a un servicio malicioso.

Y, finalmente, vemos una oportunidad para dar más especificaciones sobre el uso de los dispositivos IoT. Muchas veces la gente interactúa con los dispositivos IoT, pero no saben muy bien qué tipo de información están compartiendo con los servicios de internet, y al hacer estas consultas de DNS, los dispositivos de los usuarios generan o hacen que sean más visibles a los usuarios finales y los van a ayudar con más información interna.

En el ejemplo previo, ustedes van a ver que el reloj comparte información con el servicio remoto en internet. Muy bien, siguiente diapositiva, por favor.

Hemos visto también algunos otros ataques o botnets que se desarrollan en internet, que pueden seguir muy rápidamente y que pueden tener resolutores abiertos que pueden crear incluso un mejor tráfico. Y el otro riesgo es lo que llamamos una programación no amigable de DNS usando DNS de otra manera.

Hace unos años hubo un ejemplo donde una App de iPhone produjo una serie de consultas de DNS, por lo tanto, los resolutores utilizaron demasiado la caché y el sistema no funcionó.

Ya hemos visto esto, ya hablamos del modelo de la IoT que tenemos y que hemos discutido en el SSAC, hablamos de las oportunidades y de los riesgos. La próxima pregunta es: ¿Qué hacemos para enfrentar esos desafíos y resolver los riesgos?

Tenemos aquí una serie de desafíos para la industria del DNS de IoT, aquí vamos un poco más allá del alcance del trabajo de SSAC porque

aquí la comunidad de IoT también participa. En primer lugar, tenemos desarrollar una biblioteca de seguridad para dispositivos de IoT que brindarán estas funciones de las cuales hablábamos cuando hablábamos de las oportunidades.

La validación del DNSSEC, por ejemplo, y compatibilidad con DoH o DoT, y, además, las consultas deberían ser visibles para los usuarios finales. Después creemos que hay desafío en términos de capacitación. Capacitar a los expertos de IoT para que sepan qué es DNS, cuáles son las funciones de seguridad y qué es lo que hay que hacer para utilizarlas.

Y también para que los expertos de DNS aprendan cómo funciona IoT y también sabiendo que IoT va a cambiar la forma en que se utilizan los dominios. Esto requiere funciones diferentes para las registraciones de nombres de dominios. Los últimos dos puntos son un poco más complejos. En primer lugar, tenemos esto de trabajar en colaboración con un grupo de operadores de DNS para compartir lo que llamamos huellas de DDOS que serían como las huellas digitales de DDOS, y estos operadores deberían intercambiar la información y compartir información para estar mejor preparados.

Los operadores de DNS también deberían compartir sus capacidades para mitigar los ataques, y, además, debemos trabajar para proteger los bordes de la red contra los ataques de DDOS. Y, finalmente, sería muy interesante tener un sistema que pueda medir la evolución del internet de las cosas para ver cómo crece y cómo utiliza el DNS. Y aquí terminan mis diapositivas, Alejandra.

ALEJANDRA REYNOSO: Muchas gracias, Cristian. Y ahora vamos a continuar con el panel de expertos que van a compartir sus opiniones y sus perspectivas en este orden. Primero Eliot, segunda Lise y, finalmente, Cristian.

Les voy a presentar a Eliot Lear y a Lise Fuhr. Eliot trabaja como ingeniero de sistemas en Cisco en el área de seguridad de IoT y se centra en cómo los dispositivos y la red se comunican entre sí. En la comunidad de internet ha participado con la comunidad de IETF desde 1998, ha escrito una serie de RFCs, participa en la Junta de Arquitectura de Internet y participó en el trabajo de la restructuración de la transición de la IANA. Eliot vive en Suiza.

Lise Fuhr es la Directora General de la Asociación de Operadores de Redes de Europa desde 2016. En ETNO controla las actividades y es la representante externa de la Asociación. En nombre de la asociación ella también forma parte de la Junta Directiva y es miembro del comité de la organización de ciberseguridad de Europa.

También ha sido designada a la Junta Directiva de la ISOC desde mayo del 2019. Lise tiene más de 20 años de experiencia en la industria de las telecomunicaciones. Empezó su carrera en el Ministerio de Ciencias, Tecnología e Innovación de Dinamarca donde participó en el desarrollo de normativas para el mercado de telecomunicaciones.

Desde entonces ha trabajado en diferentes empresas de telecomunicaciones, donde ya ha trabajado en temas que tienen que

ver con servicios móviles, acuerdos de interconexión y cooperación en la industria. Eliot, usted tiene la palabra.

ELIOT LEAR: Muchas gracias, Alejandra. Próxima diapositiva.

Quisiera contarles una historia sobre un horno. Este es un horno, tiene compatibilidad con internet de las cosas. Mi prima compró uno de estos hornos, lo instaló, y un tiempo después, el horno la despertó a las 05:30 de la madrugada porque había que limpiarlo.

Personalmente eso lo considero una denegación de servicio, pero, bueno, así estaba diseñado el horno. Lo que no sabía mi prima era que para que todo eso funcione hay varios componentes que tenía este horno.

El horno no solamente tiene un elemento de refrigeración y un termostato bien aislado y todos los elementos que tienen los hornos, sino que también tiene un transductor, un CPU, memoria, algunos interruptores y un panel.

Eso representa una amenaza, es decir, cualquiera de esos componentes puede ser atacado. ¿Qué hacemos frente a uno de esos ataques? Si tenemos éxito con ese ataque podríamos ver qué pasa; pero también podemos crear un ataque coordinado. Por ejemplo, en una región donde no hay acceso, hay una especie de producción o suministro de energía especial, la pila de software.

Este software puede acceder a la limitación eléctrica de otros elementos, las radios, el aire acondicionado, muchos dispositivos pueden ser habilitados para crear una enorme demanda de consumo eléctrico. Entonces este horno causaría un problema aumentado la demanda de todos los dispositivos. La próxima diapositiva, por favor.

Para que este horno funcione… Aquí tenemos una imagen de internet, una muy buena imagen creada por KC y su equipo. El horno se comunicó con dispositivos que estaban en la nube a fin de hacer esto que dije antes, y para hacerlo así como lo hace el picaporte (la manija de la puerta) que se mencionó antes.

Fueron los dispositivos de la nube que se comunicaron con los equipos en el hogar de mi prima. Para que estos dispositivos se comuniquen con la nube, deben utilizar el Sistema de Nombres de Dominio, tienen un end point que está en la nube, que puede ser cloud.ejemplo.com y así se comunican.

Entonces para que se puedan comunicar en internet, la información debe ser enrutada por un router. En el caso del picaporte (manija de la puerta) hablamos de Wi-Fi, pero hay otras formas de lograr esta comunicación, pero gran parte de esto se comunica a través de los dispositivos del hogar, del router que está en el hogar.

Entonces, ¿cómo funciona esto? Vamos a ver, por ejemplo, una consulta del horno. La próxima diapositiva por favor. La consulta dice: “horno.nube.ejemplo.com”. Y se vuelve una dirección de IP y esta dirección de IP es algo que refiere a un dispositivo específico.

Recuerden lo que dijo Cristian, hay alrededor de veinte mil millones de dispositivos en el mundo. Hay muchos en internet, pero el horno solo tiene que comunicarse con su end point en la nube, quizás con algunos dispositivos en el hogar, pero no tiene que ver con todos los dispositivos del mundo.

Entonces si ese router hogareño puede crear un punto de control y ese punto de control limita la superficie de amenaza que puede representar ese horno, esto significa que incluso así haya un bug o una vulnerabilidad, el punto de control puede proteger el sistema de un ataque en gran escala. ¿Esto significa que el fabricante de hornos no tiene que mandar actualizaciones del software? Por supuesto que no.

Sin embargo, sigue habiendo una amenaza aún con algunas de estas protecciones de la red, pero la red ayuda a reducir las amenazas. Próxima diapositiva, por favor. Aquí tenemos la comunicación que va al dispositivo en la nube, eso ha sido resuelto por el DNS a fin de que el punto de control funcione debe recibir la consulta y la respuesta del horno. Esto significa que, si la consulta del DNS está encriptada y el punto de control no lo sabe, entonces no puede brindar protección y no puede reducir las amenazas.

La próxima diapositiva, por favor. Y, por supuesto, esto se repite con el picaporte (manija de la puerta) y otros dispositivos que usan los consumidores. En el mundo industrial las cosas son un poco diferentes. Hoy estoy hablando de los dispositivos que usan los consumidores y hay diferentes end points en las nubes utilizados por diferentes dispositivos.

¿Qué significa todo eso? Significa que está bien encriptar, hay buenos motivos para encriptar las consultas de DNS y Cristian los mencionó; sin embargo, si el router de la red que debe reducir las amenazas no puede por sí mismo tener acceso a la consulta si no está autorizado a ver las comunicaciones en términos de la consulta y la respuesta, entonces ese enrutador no puede brindar la protección necesaria. Tenemos esta vinculación entre el DNS y el enrutador que permite que esta protección sea posible, y esto se ha estandarizado, se ha buscado una forma estándar de brindar esta protección.

No estoy diciendo que no debemos encriptar, justamente, al contrario, decimos que sí hay que encriptar, pero cuando lo hacemos esto debe hacerse con un componente que esté autorizado para brindar esta protección. Y creo que esta es mi última diapositiva. ¿Alejandra?

ALEJANDRA REYNOSO: Gracias, Eliot. Ahora le damos la palabra a Lise.

LISE FUHR: Gracias. Y hola a todos. Yo voy a aportar una perspectiva diferente porque vengo del mundo de las empresas de telecomunicaciones: los ISPs.

Entonces mi presentación se va a centrar en por qué es interesante hablar de 5G y el internet de las cosas. Voy a hablar un poco de las nuevas oportunidades que se abren con el 5G, y también voy a hablar de algunos temas que preocupan en relación al 5G y al DNS. También

voy a contarles cómo creemos que va a avanzar el mundo en términos de 5G, DNS y el internet de las cosas.

Entonces si vamos a hablar del internet de las cosas, ¿por qué es interesante esto en relación con el 5G? Porque las empresas de telecomunicaciones están viendo que el 5G; que es una combinación de redes fijas y móviles, no solamente es tecnología 4G nueva, sino que es una tecnología con mucha más convergencia y vemos que esto será un componente importante para el crecimiento del internet de las cosas.

Aquí ven los números sobre la IoT móvil, quizás el número no sea muy alto y aquí decimos que en 2018 teníamos 140.000.000 de conexiones móviles de IoT, y prevemos que habrá 740.000.000 de conexiones en el año 2026.

¿Qué es lo nuevo que resultará interesante con respecto al 5G? la IoT de banda angosta, y, por supuesto, también habrá algunas mejoras MTC, que esto será en realidad un desarrollo sobre lo que ya tenemos en 4G.

Si consideramos el 5G, aquí vemos varios servicios que ya se están desarrollando en base a lo que tenemos hoy en día en 2G, 3G y 4G, que ya son compatibles con el internet de las cosas. Y el nuevo internet de las cosas será infraestructura de IP, y también infraestructura de DNS en mucha mayor medida.

En este momento lo que vemos no es lo que llamamos IoT, tiene que ver con IoT y otros servicios, y prevemos que habrá otro uso del 5G e IoT del que le estamos dando hoy en día, y creo que será en realidad un uso

mejor y más seguro. Si lo vemos como está en esta diapositiva, el IoT y el 5G no crecen en el vacío, están basados en una cartera de servicios mucho más amplias, y el DNS e IP en general, serán los que lanzarán esto.

Si miramos la herencia, vamos a ver que 5G no va a estar separado desde el día uno. Lo que vemos es que hay muchas redes que están generando una infraestructura para el 5G, entonces lo que vemos es que hay 5G con equipamiento 4G; pero no son redes 5G complemente operativas y allí el uso del DNS, los nombres de dominio y los sistemas móviles no son los más prevalentes, pero sí utilizamos mucho DNS y está limitado por ahora.

Si vemos algunas excepciones para el ruteo, VoLTE es uno de estos casos, pero ¿qué es o para qué utilizamos el DNS en los sistemas móviles? Vemos que los nombres de dominios o que el interdominio, mejor dicho, ahora está limitado y que derivan de los IDs legados, el acceso a internet móvil es no específico.

No hay nada nuevo del uso de 4G a 5G en relación con el DNS, pero lo utilizamos del mismo modo en 5G que como hicimos en 4G. Siguiente diapositiva, por favor.

Entonces, ¿por qué 5G es interesante? ¿Y por qué es más interesante que el 4G? Bueno, como dije, esto se debe a que es una red mucho más convergente, es una red virtualizada que va a utilizar mucho más software, y no va a ser tan dependiente del hardware como ocurre con el 4G.

Va a ser una red mucho más flexible, y como decimos, tiene la intención de ser nativa IP. Y, si bien es un poco difícil de operar con direcciones IPv6 porque son muy largas, todavía seguimos viendo un alto uso del DNS para esto por la estructura de IPv6.

También vemos que nuestros interdominios van a ser nativos IP, que gradualmente vamos a pasar a nombres interdominios por la forma en la que manejamos la red. En Europa todavía operamos ampliamente y nos interconectamos en base a circuitos, pero consideramos que con 5G vamos a tener mucha más interconexión IP. Esta es la forma en la que avanza la evolución sobre cómo va a ser operado el 5G. Siguiente diapositiva, por favor.

Si consideramos cómo se va a materializar el uso de los nombres de dominio, básicamente decimos que es transparente para los usuarios, en el sentido de que es invisible la manera en la que utilizamos el DNS. La forma en la que trabajamos con la red es en buena medida para cuestiones técnicas, y va a estar incluido en el dispositivo, es decir, que el uso no va a estar atado a un nombre de dominio.

El nombre no es una parte muy importante entonces de todo esto, pero la tecnología del DNS sí lo es. De nuevo, respecto de IoT y cómo se está implementando, es clave aquí porque esta implementación, esta forma de cómo implementamos es lo que define la configuración. Nosotros no creemos que 5G sea una nueva fuente de registraciones de segundo nivel, sino que más bien creemos que esto va a estar definido por subdominios.

Es decir, que no esperamos un aumento en la forma en la que utilizamos los nombres de dominio porque va a tener que ver con el uso de estos subdominios. Nuevamente, gran parte de esto no se va a resolver en internet, sino que se va a resolver como unos nombres de dominios, interdominio o intradominio. Siguiente diapositiva.

¿Por qué pensamos entonces que el 5G es beneficioso para IoT y para el DNS? Primero y principal, creemos que a nivel del núcleo de la red vamos a tener como decimos, mucho más software y que esto va a permitir y va a ser que sea mucho más flexible, que resulte más fácil trabajar con la comunicación, con una banda angosta en las máquinas. Podemos definir las redes de un modo mucho más sencillo con 5G.

Y desde el costado de la seguridad, la segmentación va a ser extremadamente importante para nosotros. La segmentación de red va a ser parte de la red donde vamos a poder definir un uso específico, por ejemplo, los autos o los coches automáticos que son el futuro de IoT, van a requerir de una latencia muy baja y allí entonces va a ser muy importante que tengamos un tipo de servicios para los autos o los coches automáticos.

También el uso de la inteligencia artificial, creemos que va a optimizar la red tanto para mejorarla, como para ayudarnos a encontrar amenazas o problemas con la red. Creemos entonces que la inteligencia artificial nos va a permitir trabajar más rápidamente y nos va a permitir también encontrar cuáles son los problemas posibles.

Volvemos entonces a los desafíos en la siguiente diapositiva. Si consideramos lo que nosotros vemos como desafíos y cómo podemos mitigarlos, pensamos que la segmentación de red es extremadamente buena, ha habido cierta inquietud de que esto pueda crear una fragmentación de internet. Nosotros no vemos que haya ningún inconveniente con esto, más bien lo vemos como VPNs, son servicios mucho más dirigidos a los usuarios a finales y no van a crear ninguna fragmentación de internet.

Si miramos los nombres de dominios y el evitar las colisiones, utilizamos los dominios públicos y no lo vemos como un problema. Si es que existe un dominio que utilizamos para el enrutamiento interno, va a haber un dominio público y no se va a crear aquí ninguna colisión.

Respecto del DNS que es algo que nos parece importante, el DNSSEC va a ser una oportunidad. No es un estándar obligatorio por el momento en el 5G, todavía no hemos visto nada que pueda llegar a crear una necesidad para que el DNSSEC se convierta en un estándar en la red de 5G, pero nos parece que sí se debe utilizar.

Y, nuevamente, respecto de la denegación de servicios, los ataques de DDOS y los botnets en las redes 5G, por supuesto, que lo podemos manejar, pero existe una atendencia a la encriptación y si quieren monitorear estos ataques tenemos que poder ver el tráfico. En la denegación de servicios, si somos una parte activa en esta defensa debemos poder ver el tráfico. Siguiente diapositiva, por favor.

¿Cómo continuamos entonces? Todavía hay muchas preguntas abiertas respecto de la estandarización del 5G. Estamos generando estas redes 5G y no hemos visto hasta ahora ninguna red independiente es 5G, como decía, por ahora es el 4G con componentes del 5G, la infraestructura sigue siendo costosa.

Como dije, el 5G todavía no está aquí a la vuelta de la esquina, no es independiente y estas redes son extremadamente caras. Una última cuestión, es que vimos que la crisis del COVID que ha sido una crisis terrible para todos nosotros. Vimos en todo el mundo que hay un foco muy sólido para la necesidad de la digitalización, hay un foco también en la seguridad, y desde esa perspectiva vimos que hay una conciencia creciente de que la infraestructura es importante.

La seguridad es importante, y también que hay un aumento en el uso de nuestras redes, es decir, que nosotros lo que vemos es que el futuro nos va a traer un muy buen ejemplo. Vemos aquí que ninguno de nosotros viajó a una reunión de ICANN y, en lugar de eso, lo estamos haciendo en forma remota.

Y en cuanto al IoT, el internet de las cosas, lo vemos como un resultado también de esta crisis, es decir, se va a crear más monitoreo remoto y más IoT. Esta fue mi parte, muchas gracias.

ALEJANDRA REYNOSO: Muchas gracias, Lise. Y ahora le vamos a dar la palabra a Cristian.

CRISTIAN HESSELMAN: Muchas gracias. Voy a cambiarme el sombrero, antes estaba usando mi sobrero de SSAC y ahora voy a usar mi sombrero de .NL.

.NL es el registro para los Países Bajos, somos un país pequeño en Europa, la semana pasada llegamos a los 6.000.000 de dominios, ese es un motivo para celebración.

Una de las cuestiones importantes que hacemos es que queremos mejorar la seguridad y la resiliencia de internet, como pueden ver en la diapositiva, y por eso hace un par de años decidimos empezar a trabajar en el internet de las cosas, específicamente para hablar de algunos de los desafíos que mencioné antes cuando hablamos de las oportunidades, riesgos y retos como parte de esta presentación.

Y la razón es que el ataque Dyn que ocurrió, el operador de DNS fue atacado por un botnet que envió muchísimo tráfico. El botnet tiene cientos de miles de dispositivos IoT infectados y envía mucho tráfico, y como resultado ocasiona cortes en servicios como Twitter, Spotify y otros.

Cuando lo vimos, dijimos: “Somos un operador de DNS, somos infraestructura crítica para los Países Bajos y para internet en general”. Y por eso tenemos que hacer algo. Allí es donde empezamos a desarrollar el protocolo SPIN. SPIN significa seguridad y privacidad en redes internas y el objetivo del sistema es básicamente monitorear, es decir, uno coloca un dispositivo en la red para mejorar el Gateway hogareño con seguridad adicional y esta funcionalidad de seguridad va a monitorear la red local para ver si hay tráfico de DDOS.

Los dispositivos IoT entonces que tenemos en el hogar, si van a estar infectados por un botnet, van a participar en una de estos ataques de DDOS. Entonces tratamos temporariamente de desconectar ese dispositivo de internet para poder proteger la infraestructura de internet de este ataque de DDOS.

Es como un firewall inverso. Aquí vemos un ejemplo de algo que desarrollamos en SIDN, es decir, que este sistema está en etapa de prototipo. Si bien el año pasado invertimos en software para llevarlo a un nivel de producción, y lo que queríamos era poder ayudar a los ISPs y poder ayudar a los fabricantes de dispositivos para consumidores a que utilicen estas funciones en el dispositivo, pero esto terminó siendo mucho más difícil de lo que pensábamos por los diferentes ecosistemas del DNS que utilizamos, y también es un ecosistema comercial diferente.

Los ISPs, al menos aquellos de lo que hablamos no se explican, ¿cómo ayudar a nuestros clientes a resolver problemas con dispositivos IoT que no estaban certificados? Entonces todos son un poco renuentes, por este tipo de servicios adicionales que pueden generar una carga y que pueden introducir un costo adicional.

Esto es entonces uno de los factores que tienen que ver con la implementación de todo esto. Otro factor es el de los fabricantes. Se deben agregar todas las funciones, es decir, que hay un problema del huevo y la gallina aquí.

Nosotros sabemos que este es un problema importante porque al menos en Europa si miramos el regulador de telecomunicaciones nacionales, ellos tienen un programa específico para seguridad IoT, y también hay una iniciativa europea, donde hay distintos reguladores de Europa que tratan de extender la narrativa de las radios a cualquier otro dispositivo que tenga radio transmisión y extender esa especificación a los requisitos IoT específicos.

Es decir, que hay un problema importante desde la perspectiva pública, pero hay más tracción en la industria, especialmente en el mundo de los ISPs; el mundo de la conectividad debería decir. Siguiente diapositiva, por favor.

El software que vieron recién es código abierto, y otro ejemplo de los mismos prototipos que desarrollamos… Acá vemos la transparencia, recuerden que anteriormente hablé de la oportunidad del DNS de visualizar las consultas por partes de los usuarios de una forma simple e intuitiva. Desarrollamos prototipos para ilustrar esto, es lo que ustedes están viendo en esta pantalla.

Entonces, básicamente, los círculos grises son dispositivos que están en la red. El que está arriba creo que es el teléfono y tiene muchos dispositivos conectados con él; y los que están en azul y en verde son básicamente servicios remotos con los que se conectan estos dispositivos. Esta es una captura de pantalla, la aplicación propiamente dicha es muy dinámica. Pueden ver las interacciones con los servicios remotos que van apareciendo a medida que se presentan.

Este es el análisis de las consultas al DNS, y debería agregar que es una solución amigable en términos de privacidad porque conserva todas las mediciones y los análisis dentro de la red, no lo comparte con servicios de nube y ese tipo de cosas.

Estos son dos ejemplos de sistemas con lo que estamos tratando de resolver los desafíos, que mencionamos en el informe del DNSSEC, y tenemos un ejemplo más en la próxima diapositiva.

Este último ejemplo tiene que ver con lo que la ISOC llamó seguridad colaborativa. Múltiples organizaciones trabajan en conjunto para brindar más seguridad a internet, lo cual es básico para internet porque internet es una gran fuente de colaboración. Tenemos que trabajar juntos, y uno de los ejemplos en los que trabajamos, es lo que llamamos la cámara compensadora de DDOS.

Permite que la gente comparta resúmenes de ataques que observan en sus sistemas, reciben tráfico entrante, generan una huella digital y comparten esa huella digital con otros operadores dentro del grupo para que estos otros operadores sepan que se están produciendo este tipo de ataques y puedan prepararse y preparar su infraestructura con anticipación, en caso de que el ataque apunte a ellos.

Se trata de ser proactivos. Para la víctima ya es demasiado tarde, sigue siendo reactivo, pero para los demás miembros del grupo es proactivo porque cuentan con más información acerca de este ataque que les ocurrió a otros proveedores de servicios. Esta es básicamente la capa

de información que se agrega por encima de la infraestructura de mitigación de ataques de denegación de servicios.

Es un sistema distribuido que se agrega en la capa superior, y esto es algo que estamos probando a modo piloto en los Países Bajos, hay un nomoreddos.org, ahí tienen un vínculo que les lleva a un blog con la información adicional. Actualmente estamos haciendo un programa piloto en Holanda que forma parte de un proyecto europeo más amplio, CONCORDIA, y se trata de estas cámaras compensadoras de DDOS.

Tenemos entonces un trabajo a nivel nacional, los miembros o las organizaciones de Holanda, los gobiernos, los ISPs, los intercambiadores de internet. Muchas organizaciones trabajan en este proyecto, pero también es posible organizarlo de una forma diferente, si también podríamos imaginar una cámara compensadora de DDOS para la industria de DNS.

Los operadores de DNS a nivel de registro y registrador pueden colaborar para compartir información acerca de estos ataques. Estos son básicamente tres ejemplos que quería darles desde la perspectiva de nuestro trabajo y que podría quizás ayudarlos a resolver o a enfrentar los riesgos y aprovechar las oportunidades que mencionamos en el informe del SSAC. Muchas gracias.

ALEJANDRA REYNOSO: Muchas gracias, Cristian. La próxima diapositiva.

Ahora llegamos al momento de la revisión por parte de pares. Tenemos a Philippe Fouquart, que es un representante del ISPCP de la Unidad Constitutiva. Philippe es experto sénior en nombres, números y direcciones en las redes At-Large.

Desde 2001 ha estado a cargo de estas actividades en Orange Labs y brinda soporte técnico en esta área a las unidades de negocios dentro de todo el grupo.

Rafik Dammak, es ingeniero informativo que vive en Japón y está terminando su maestría en ciencias informáticas en la Universidad de Tokio.

Trabajó en temas de gobernanza de internet desde 2007, trabaja en foros de internet y en otras conferencias de internet como orador o como organizador. Su área principal son los procesos de desarrollo de políticas. Ha trabajado en diferentes funciones, en la Unidad Constitutiva de Usuarios no Comerciales, NCUC y en el grupo de partes interesadas no comerciales.

Y también genera concientización acerca de temas de gobernanza de internet en la región.

Kimberly “KC” Claffy es directora del Centro de Análisis Aplicados de Internet en la Universidad de California en San Diego. En 2017 recibió el premio Jonathan B. Postel Service, también es profesora adjunta en el departamento de ingeniería de ciencias informáticas en la Universidad de San Diego.

Sus temas de interés abarcan topología de internet, routing, seguridad, futura adquisitoria de internet y políticas. Trabaja en SSAC desde 2003 y también trabaja en la Universidad de California en San Diego en ciencias informáticas. Les doy la palabra.

Podemos comenzar con Philippe.

PHILIPPE FOUQUART: Gracias, Alejandra. ¿Me escuchan?

ALEJANDRA REYNOSO: Perfectamente.

PHILIPPE FOUQUART: Gracias, y gracias a los panelistas. Algunos mensajes y quizás un comentario. Eliot habló acerca de casos de usos en donde se utiliza un dispositivo que se conecta con un marco y no dispositivo a dispositivo. Eso sería como un Gateway de IoT para que la red local no esté totalmente ciega a los pedidos de DNS entrantes y salientes.

De esta forma, se puede reducir una serie de amenazas de seguridad. Debemos diferenciar entre las dos dimensiones, una es IoT en internet móvil y las aplicaciones y servicios de IoT brindados por un operador. Y también la segmentación que no es una amenaza, hay arquitecturas que se utilizan ya en las redes móviles y son diferentes de la que conocemos con DNS en internet.

Y, finalmente, Cristian habló acerca de un concepto piloto de un Gateway de IoT para monitorear el tráfico saliente como forma de combatir estos ataques de denegación de servicios. Esos son mis mensajes principales que rescaté de las presentaciones. Tengo un comentario o pregunta con respecto a los desafíos.

IoT es un ecosistema muy complejo que quizás no forme parte del trabajo de aquellos que definen los estándares, quisiera saber cómo se puede desarrollar protocolos en general y para DNS en particular, y cómo se conectan con esta comunidad de actores. Entonces quizás esta sea una pregunta o un comentario para que lo consideren los miembros del panel.

Me gustaría saber más acerca de en qué parte del ecosistema está, si son operadores, registros. ¿Cómo podemos conectarnos o cómo pueden ustedes conectarse con esa comunidad de fabricantes de dispositivos para promover esas buenas prácticas? Gracias.

Alejandra, te doy la palabra.

ALEJANDRA REYNOSO: Gracias, Philippe. Con respecto a sus preguntas, creo que los expertos las van a pensar. Vamos a darles la palabra a los otros revisores y al final vamos a ver si podemos responder las preguntas. Le doy la palabra a Rafik.

RAFIK DAMMAK: Gracias, Alejandra, y gracias a los miembros del panel por sus presentaciones. Yo también rescato algunos mensajes y quisiera decir que uno de los mensajes importantes es que parece estar fuera del mandato de ICANN, pero quisiera saber qué es lo que el ecosistema le puede dar a IoT. Lo que observé es que hablamos acerca de los diferentes actores IoT, el ecosistema y los diferentes actores, y acerca de lo que tienen que hacer para mejorar la seguridad.

Lo que no me quedó claro es cuál puede ser el rol del usuario. Quizás no sea una respuesta directa, pero ¿qué esperamos del usuario final? ¿Qué necesitamos por parte de ellos? Como consumidores usuarios de diferentes tecnologías, a veces ellos se ven afectados también por estos ataques a IoT y a los otros dispositivos.

Y a veces se ven afectados por IoT, aun cuando no sean consumidores directos. Cristian habló acerca de cómo tenemos que ayudarnos en cuanto a utilizar sabiamente el DNS y las mejores prácticas, y yo me pregunto a partir de la experiencia en la ICANN cuando se introdujeron los nuevos gTLDs y los IDNs, tuvimos esa experiencia con respecto a la Aceptación Universal.

Me pregunto si esto podría ser útil o adecuado en términos de lecciones aprendidas o abordajes que podrían aprovecharse para ayudar a informar acerca del mejor uso o las mejores prácticas con respecto al DNS en el contexto de IoT. Quizás Cristian basándose en su propia experiencia y en el trabajo del desarrollo de .NL, quizás él podría decirnos si hay algunas áreas comunes y algunos aprendizajes que podríamos tomar de esa experiencia.

Y otro punto, creo que fue bueno escuchar acerca del contexto de IoT y aprender quizás cómo se utiliza en esta área, pero quisiera saber si podría hablar un poco más acerca de si hay alguna área de política que tenemos que tener en cuenta con respecto a 5G. Eso es todo.

ALEJANDRA REYNOSO: Gracias, Rafik. Como dije, vamos a darles la palabra primero a todos los revisores y luego vamos a responder las preguntas. KC.

KIMBERLY "KC" CLAFFY: Muy buenas presentaciones, y estamos viendo que se está volcando mucho esfuerzo al DNS. Quisiera saber qué saben los oradores acerca del apoyo del gobierno a estas actividades. En Estados Unidos hemos estado trabajando en esta área desde hace años con el fin de ayudar a la industria a anticiparse a estos problemas.

Lo que veo es que el movimiento de IoT nos está obligando, o nos va a obligar, a confrontarnos con la incapacidad para resolver muchos de los desafíos de seguridad fundamentales que estamos viviendo en la arquitectura de internet. Y dedicamos mucho tiempo y energía a desarrollar tecnologías como DNSSEC.

Y las organizaciones de normas y estándares tratan de desarrollar un protocolo que nos permite resolver el problema de seguridad, pero lamentablemente todavía no lo hemos logrado. Hay abordajes alternativos que se han intentado como, por ejemplo, el espacio de BGP. Se ha trabajado en el área de enrutamiento y seguridad con una

especie de código de comportamiento en el mundo de ISP, si ustedes hacen estas cosas vamos a reducir los ataques, etc.

Pero en última instancia no hemos logrado encontrar los medios técnicos. Quisiera saber si podrían hablar un poco más acerca de si piensan que algo así es viable en el espacio de IoT, dado que en el espacio de IoT ni siquiera es opción crear una capa técnica, la capa que hemos tratado de crear en el área de enrutamiento, debido a que hay tantos protocolos de IoT interoperables. Quisiera saber qué opinan al respecto.

Eso es todo lo que quería decirles. Muy buenas presentaciones. Voy a poner los URLs en el chat.

ALEJANDRA REYNOSO: Muchas gracias, KC. ¿A cuál de los especialistas o de los expertos les gustaría comenzar?

ELIOT LEAR: En primer lugar, todos los revisores marcaron puntos muy importantes, gracias, y hallé muy buenas conversaciones en la sala del chat, un debate muy dinámico. KC, tiene toda la razón, hemos dedicado mucho tiempo y esfuerzo a resolver los desafíos de seguridad de IoT. Por ejemplo, tenemos el NIST TR8228 que habla acerca de las consideraciones de manejar internet de las cosas, prácticas de ciberseguridad y riesgos.

Y también la recomendación preliminar SP1800-15, que habla acerca de los ataques de denegación de servicios en IoT, con un foco en la descripción de uso de fabricantes. Hay un punto y es que, IoT es una especie de nebulosa, toca diferentes áreas verticales, hablamos mucho de los consumidores, pero también tenemos la parte industrial, ciudades inteligentes, hogares.

Es importante reconocer que muchos de estos sectores ya están muy regulados. La FDA regula todos los dispositivos médicos y terapéuticos, independientemente de que tengan conectividad a internet o no están regulados, y ellos seguramente tendrán mucho que decir con respecto a la seguridad del dispositivo. Y lo mismo se aplica a otras infraestructuras críticas, la IoT también afecta a la industria nuclear, muy regulada.

La pregunta es: ¿Qué clase de regulación o mejores prácticas se necesitarán para algunas de las otras áreas en donde estamos viendo uso indebido? E incluso los consumidores tienen un espacio regulado. Muchas gracias.

ALEJANDRA REYNOSO: Muchas gracias, Eliot.

LISE FUHR: Quiero preguntarle a Philippe sobre los distintos actores. Creo que la cooperación o el informe del SSAC es un muy buen ejemplo sobre cómo nosotros podemos volver al modelo de negocio a negocio de nuestros

clientes y también a los gobiernos, y discutir las buenas prácticas y ver de qué manera hacer que tengamos más seguridad.

Me parece que el diálogo entre ICANN y SSAC en Europa, tenemos también a ETSI, creo que es importante. Se debe hacer esta especie de mezcla, lo estamos haciendo nosotros con los usos. A Rafik, respecto de si hay alguna política en DNS y el 5G, hay muchas políticas en cuanto a la seguridad y el 5G en Europa.

Tenemos una nueva ley de seguridad que también tiene relación con el 5G y no es específica de DNS, pero creo que cuanto más esté desarrollado el 5G más foco va a tener en como el DNS y el IoT está teniendo en cuenta el área de la seguridad. Y tenemos lo que llamamos un toolbox, una caja de herramientas de seguridad del 5G que tiene mucho que ver con los dispositivos; pero me parece que es una regulación muy importante que debemos tener en cuenta con respecto a las áreas del DNS.

Respecto de lo que dijo KC y la imposibilidad de resolver los problemas de seguridad, es cierto, hay un movimiento constante hacia cómo nos ocupamos de la seguridad porque la tecnología avanza muy rápidamente.

En Europa tenemos ENISA, que es un organismo del lado de la comisión, y ellos ahora han establecido un grupo de partes interesadas de seguridad donde se habla de la estandarización en relación con la seguridad, y estoy segura de que también se van a incluir áreas del IoT y del DNS. Gracias.

ALEJANDRA REYNOSO: Muchas gracias, Lise.

CRISTIAN HESSELMAN: Quería responder a lo que dijo Rafik. Obviamente, los usuarios son una parte importante de la ecuación porque para eso estamos. Creo que tenemos que empoderar a los usuarios para que comprendan mejor qué es lo sucede en el IoT y que conozcan más qué ocurre cuando interactúan conscientemente con un dispositivo IoT, que puede tener una visualización o algún otro tipo de representación de la información importante que estamos compartiendo con los servicios remotos en internet.

Y esto puede iniciar una discusión o una demanda de clientes si tenemos soluciones de seguridad en las cuales el DNS puede tener un rol. También desde la perspectiva del ciudadano, que es la del usuario final, creo que los gobiernos y otros organismos tienen que jugar un papel también. Estábamos viendo ya eso especialmente en los Países Bajos donde el regulador tiene un rol, en Estados Unidos también lo vemos, en los equipos de radio.

Hablé también de la regulación europea, y sobre eso, creo que en cuanto a la política los gobiernos y quizás ICANN como generador de políticas, pueden fijar un estándar para el nivel mínimo de ciberseguridad que debe haber en los dispositivos. Gracias.

ALEJANDRA REYNOSO: Muchas gracias, Cristian, y a todos. Y ahora vamos a pasar a las preguntas que se han insertado en la sección de preguntas y respuestas. Recuerden utilizar el recuadro de preguntas y respuestas. El chat no se va a leer en voz alta.

Muy bien. ¿Cómo estamos entonces con las preguntas, Ria?

RIA OTANES: Gracias, Alejandra. Tenemos una pregunta de Angie Matlapeng: "¿Ha habido cuestiones de memoria que fueron presentadas por IoT o dispositivos IoT más pequeños, en relación con la utilización del DNSSEC y la encriptación para proteger esos dispositivos?"

ELIOT LEAR: Quizás yo pueda responder.

ALEJANDRA REYNOSO: Adelante.

ELIOT LEAR: Gracias por la pregunta, Angie. IoT tiene algunos retos en relación con memoria, obviamente cuando hablamos de los dispositivos de consumidores y otros dispositivos más pequeños, en particular la memoria es algo Premium. He tenido debates con desarrolladores de IoT.

Y si miramos las pilas que ellos utilizan, hay pilas especializadas de encriptación, OV SSL es un buen ejemplo donde tienen pilas de encriptación muy específicas y uno puede tener mucho más de un megabyte en tamaño, mientras que hablamos de 14 kilobytes en otros casos. Como para darles una idea de las diferencias.

Pero hay otras cuestiones vinculadas con el IoT, que es que estos dispositivos, como alguien dijo antes, lo dijo Cristian creo en su introducción. Duran mucho tiempo y el mundo de la encriptación cambia con los años, y lo que nos pareció que era una encriptación aceptable hace cinco o diez años, es altamente vulnerable a los ataques.

Y si pensamos en dispositivos como plataformas petroleras, lo ponemos en la tierra durante 40 años. Recuerden lo que teníamos hace 40 años en términos de tecnología y ahora, imagínense tratar de actualizar un dispositivo para utilizar la tecnología actual, un dispositivo que ya tiene 40 años, imagínense actualizarlo…

Este es un gran reto para IoT, y no hay soluciones simples. Una persona, creo que es alguien de M.I.T, escribió un documento muy interesante donde sugería que los dispositivos IoT tienen un switch que ya no están más en la red, hay veces en que es posible y hay veces en que no, pero es algo para pensar.

ALEJANDRA REYNOSO: Muchas gracias, Eliot. Creo que tenemos una pregunta más.

RIA OTANES: Es de Anupam Agrawak: "¿Cree usted que el sistema de identificadores existentes va a poder cumplir los requisitos de privacidad en el caso de IoT?"

ELIOT LEAR: Creo que el silencio es porque es muy difícil de responder. Adelante, Cristian.

CRISTIAN HESSELMAN: Bueno, ya hablamos de esto, hay dos partes. Una parte es la de los identificadores que, en este caso, es el nombre de dominio como identificador. Esto se puede proteger para aumentar el uso de la privacidad. Hemos hablado de eso anteriormente en nuestra charla, y, por supuesto, hay una segunda dimensión que es, ¿qué tipo de información están compartiendo esos dispositivos con los servicios remotos?

Es decir, puede haber un contenido, pero puede haber patrones de tráfico. Algunas investigaciones han establecido que la gente puede evaluar qué tipo de dispositivo va a tener en su casa, solamente al ver el patrón del tráfico y no el contenido se puede ver cuál es el dispositivo que se tiene en la casa.

Hay muchas dimensiones, tenemos que ver la protección del sistema de identificadores, el DNS, pero también el tráfico real de los servicios remotos que van o que se reciben, y hay que proteger esa información

en términos de encriptación e incluso también en términos de cómo vamos a ocultar lo que el dispositivo está haciendo en el servicio remoto.

Estoy de acuerdo con Eliot de que es una pregunta complicada.

ALEJANDRA REYNOSO: Muchas gracias, Cristian. Eliot, no sé si quiere decir algo más.

ELIOT LEAR: Quería responder la pregunta de Nigel. Él nos preguntó sobre los desafíos en los mecanismos de 5G e IoT en el mundo estándar.

Yo creo que sí hay retos para el 5G, el principal es cómo vamos a limitar la superficie de estos dispositivos. ¿Cuál es el rol del proveedor en limitar esta superficie de amenaza? Es decir, ¿cuál es la interacción entre el control de la red que es un paquete y el DNS en un mundo de nube?

Son las mismas cuestiones que ocurren en la casa o en el hogar y que deben tener en cuenta la red de 5G. Estas discusiones las tuvimos incluso al principio, ¿verdad?

ALEJANDRA REYNOSO: Muchas gracias, Eliot. Vamos a tener una última pregunta porque nos estamos quedando sin tiempo lamentablemente. Ria.

RIA OTANES: Tenemos una pregunta de Suada Hadzovic: “Si tenemos proveedores de nube de IoT, ¿cuál es la relación con NIST, Edge o Fog? Según el NIST, los nuevos Fog son componentes físicos como los Gateways, etc.

ELIOT LEAR: Gracias, voy a tratar de responder. Hay distintos modelos computacionales para los dispositivos IoT. Como dije en una de las respuestas, el costo de los bienes y servicios en el nodo real, hay muchos que tratan de mantenerlo muy bajo, pero a veces lo que hacen es que cambian la potencia y si el fabricante tiene que agregar más, a la nube le resulta muy bueno.

Pero ¿cómo podemos tener algunas limitaciones? Las puede haber en la latencia cuando necesitamos capacidades locales y esta es la noción de la computación en nube. Esto es un área, diría yo, que tiene que tener más exploración. No es algo que veríamos en el espacio del consumidor, pero veremos mucha computación de nube en el espacio industrial donde tenemos controladores locales que tienen capacidades adicionales en términos de procesar localmente y coordinar la comunicación entre los dispositivos IoT.

Hay mucho de esto en el espacio industrial, pero también es un área que es muy flexible y que se debe explorar.

ALEJANDRA REYNOSO: Muchas gracias, Eliot. Con esto voy a cerrar la sesión. Les voy a dar unas pocas oraciones.

Es muy importante para nosotros que la conversación continúe, en relación con las oportunidades, riesgos y retos, y la interacción del DNS y el IoT. Es importante saber que hay una interacción, que los usuarios no conocen lo que ocurre con sus dispositivos y es algo en lo que hay que trabajar.

La privacidad es un tema, la seguridad también lo es. Hay algunos desafíos en ese sentido y el trabajo que podría hacer la comunidad de la ICANN es entender un poco más los riesgos y los desafíos, y de qué manera las distintas organizaciones comunitarias y comités asesores pueden contribuir a que exista una mejor interacción entre el internet de las cosas y el DNS.

Quiero agradecer a todos los panelistas y a los revisores por su tiempo y colaboración, y al personal de la ICANN que nos ayudó en esta reunión plenaria. Muy buen trabajo. Esta plenaria ha llegado a su fin, muchas gracias a todos por su asistencia y nos vemos en la próxima. Hasta luego.

[FIN DE LA TRANSCRIPCIÓN]