lanacion.com

Sábado 18 de julio de 2015 | Publicado en edición impresa
La compu

Espiar Internet equivale a atacar el sistema

rres | LA NACION SEGUIR

En general, usamos la Red sin pensar en cómo funciona. Está ahí y ya. Sin embargo, existe un grupo de hombres y mujeres -en su mayoría voluntarios- que hacen que Internet ande, que esté ahí y ya. Forman parte de la IETF, por Internet Engineering Task Force (Fuerza de Tareas de Ingeniería de Internet), que da origen a los estándares de la Red, en particular los relacionados con el paquete de protocolos TCP/IP.

Hace casi exactamente un mes, otra de las organizaciones relacionadas con los mecanismos internos de la Red, la Corporación para la Asignación de Números y Nombres de Internet (Icann, por sus siglas en inglés), hizo su quincuagésima tercera reunión aquí, en Buenos Aires, y entonces tuve la oportunidad de sentarme a charlar con el finlandés Jari Arkko, Chair de la IETF (un cargo equivalente a presidente, aunque en la IETF tienden a evitar esos formalismos). Estuvo también con nosotros Barry Leiba, que además de trabajar en Huawei, colabora con la IETF en aplicaciones y estándares relacionados con la seguridad.

"El principal motivo por el que estamos aquí -arrancó diciendo Arkko- es que se está realizando una reunión de la Icann y, aunque no somos Icann, estamos juntos en el traspaso de algunos de los roles del gobierno de Estados Unidos en el mantenimiento de Internet a una comunidad formada por la Icann y la IETF (http://www.lanacion.com.ar/1674480), y esa es la razón por la que tanta gente ha venido a participar de ese proyecto conjunto esta semana. Para nosotros es un lugar genial, Buenos Aires es una hermosa ciudad, pero, además, en abril de 2016

vamos a tener una reunión de IETF aquí. Va a ser la primera vez en América del sur.

-¿Por qué por primera vez? ¿Por qué no vinieron antes?

Jari Arkko: -Tendemos a ir a lugares de donde son los participantes originalmente. Hace 10 o 15 años eran de Estados Unidos y Europa. Recientemente, Asia se ha convertido en una fuente importante de tecnología de Internet. Así que hemos viajado mucho ahí. Ahora vemos una participación creciente de América latina, y queremos estar aquí. Pero, además, queremos estar abiertos a diferentes tipos de organizaciones: la academia, los fabricantes, operadores, los gobiernos, los reguladores. Estamos aquí para todos, no para un grupo selecto. Esa es nuestra meta, y las reuniones son sólo una parte de la cuestión.

-¿Tradicionalmente, América latina no ha contribuido significativamente a la tecnología de Internet, o sí?

J.A.: -La participación está creciendo. En algunos casos los participantes no están viviendo en la región actualmente, pero son originalmente de aquí.

Cristian O'Flaherty, que trabaja para Global Crossing y es gerente senior de educación de la Internet Society (www.internetsociety.org), y que también está con nosotros en la charla, pone ejemplos: "Los que se están desarrollando en América latina no son los protocolos más populares, como HTTP o IP, pero, por ejemplo, la Argentina es muy activa en tecnologías de seguridad". Por su parte, Leiba acota: "Nosotros registramos de dónde vienen las contribuciones, en términos de quiénes publican propuestas y de quiénes vienen a las reuniones. Por ejemplo, en el caso de China, primero el interés y la participación crecieron, y luego eso se tornó en la publicación de estándares importantes. En el caso de América latina estamos viendo la misma curva de crecimiento, con el aumento del interés y la participación en las reuniones, quizás con 30 o 40 personas". "Ahora hay más personas en las reuniones, pero la mayor parte de la participación es por medio de listas de correo, y eso es difícil de medir", observa O'Flaherty.

-Tengo aquí anotadas varias preguntas. Esta no es quizá la más importante, pero su perfil en la IETF dice que usted se comunica usualmente con su lavarropas por medio de Facebook. ¿Qué significa eso? [risas]

J. A.: -Déjeme explicarle. Buena parte de la gente que trabaja en la IETF es

voluntaria. Yo trabajo para Ericsson Research, en Finlandia, donde me ocupo de la Internet of Things (IoT; https://es.wikipedia.org/wiki/Internet_de_las_cosas), por medio de prototipos y esa clase de cosas. Pero antes de empezar con esa tarea ya era un hobbista que fabricaba toda clase de cosas que suenan bastante locas, y eso me dio una experiencia de primera mano de lo que funciona y lo que no. Una de esas cosas que probé es una suerte de interfaz social para la IoT, que resulta más fácil para mí, como humano, porque recibo los mensajes dentro del mismo flujo de posts donde leo todo lo demás.

-Querría aclarar algo que es poco conocido de Internet. ¿Es cierto que cualquier persona puede proponer un RFC (https://es.wikipedia.org/wiki/Request_for_Comments**) y, de ese modo, expandir las posibilidades de Internet?**

J. A.: -Sí, eso es así.

-Cómo se hace eso. ¿Se envía un mail?

J. A.: -Una forma es unirse a una lista de correo, ver si otros tienen una necesidad o un problema similar (si es algo muy específico, como lo mío con el lavarropas, probablemente no prospere), y de ahí en más avanzar con el desarrollo. Lo hermoso de Internet es que cualquiera puede construir cosas sobre ella sin pedirle permiso al gobierno o los operadores de redes o tu madre.

-Pero eso está en parte cambiando.

J. A.: -Me atrevería a decir que no.

-Lo diré de otra forma: existe cierto peligro de que ese estado de cosas cambie.

J. A.: -Hay cierto peligro, sí, algunas amenazas a la innovación sin permiso. Pero a la vez están ocurriendo ciertas cosas, como lo que está haciendo Barry con la comunicación en tiempo real usando el browser, algo que antes estaba reservado a Skype y otras compañías que estaban en condiciones de proveer Voip (https://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet) y videoconferencia. Y ahora cualquiera con un navegador puede hacer lo mismo. Lo mismo estamos haciendo con la IoT, de modo que no tengas que construir una red aparte para comunicarte con tu tostadora o con lo que quieras comunicarte.

-Estaba pensando más bien en la concentración (YouTube, Facebook, Netflix). Me pregunto cómo haría una startup, como lo fueron en su momento Google o Facebook, para crecer en el entorno actual.

Barry Leiba: -Cuando YouTube permitió que la gente subiera videos eso fue algo nuevo, algo que la gente antes no podía hacer. Se les ocurrió la idea, crearon el sistema y lo pusieron en línea y se volvió popular. La clave aquí es traer una idea de algo que a la gente le va a interesar. Creo que no hay ningún peligro de que eso deje de ocurrir, mientras tanto mantengamos disponible el modelo de innovación sin permiso. El hecho de que Google haya crecido tanto y ofrezca tantos servicios y esté en todas partes no limita el que otro tenga una idea y la implemente.

-Debo suponer que la IETF está a favor de la neutralidad de la Red.

J.A.: -La neutralidad de la Red es un asunto significativo. La IETF ha discutido eso, pero lo que nosotros hacemos es asegurarnos de que los servicios y protocolos que estamos desarrollando estén disponibles para todos. Estamos tratando de esclarecer de qué forma la administración de la Red puede funcionar de una manera neutral y estamos recomendando esos mecanismos. Lo que no podemos es forzar a nadie a trabajar de una cierta forma. Pero sí queremos proveerles las recomendaciones y destrezas para que operen de una forma neutral.

-¿Qué opinan de la última decisión de la FCC sobre la neutralidad (http://www.lanacion.com.ar/1765804-proponen-que-internet-sea-un-servicio-publico)?

-La IETF per se no tiene una opinión sobre el tema de la neutralidad. Uno de los problemas al analizar la neutralidad es que resulta demasiado fácil ponerla en términos de blanco y negro. En la práctica hacen falta tomar decisiones, y eso hace que no sea una cuestión de blanco y negro, como las discusiones comerciales y políticas suelen hacerla parecer. Soy optimista en que vamos a seguir teniendo el modelo de innovación sin permiso en el futuro.

-OK, hablemos de su trabajo en lugar de política [risas]. Internet es vista como algo que no tiene una vulnerabilidad que permita que se la apague. ¿Esto es así?

B. L.: -Eso es mayormente así, sí.

-¿No hay ninguna gran debilidad en Internet?

J. A.: -Déjeme mencionarles dos cosas. Hace unos años me preocupaba que Internet fuera demasiado estable, que no pudiéramos cambiar nada importante, que siempre íbamos a tener IPv4 (https://es.wikipedia.org/wiki/IPv4) y TCP (https://es.wikipedia.org/wiki/Transmission_Control_Protocol) y las mismas versiones de todos los protocolos, y que no pudieran hacerse cambios fundamentales. En los últimos dos años he visto que eso no es así, que hay una enorme cantidad de innovación en el área de la Web, que acaba de lanzar el protocolo HTTP/2 (https://es.wikipedia.org/wiki/HTTP/2), que es el primer gran rediseño en su historia, y ya estamos pensando en lo que viene después, HTTP/3. Y también estamos viendo cómo reorganizamos todos los demás protocolos. Por ejemplo, TCP, ¿hace sólo control o debe hacer también seguridad? Pensamos en cómo combinar las cosas que tenemos hoy de nuevas formas. Así que esa debilidad no es tal.

-¿Y la otra?

J. A.: -La otra es la seguridad. Cuando hablamos de seguridad en Internet parece ser algo banal; si hacemos Internet más segura, todos van a estar felices. Pero no es tan simple. Es un asunto enorme, es muy complicado y tiene componentes técnicos, pero también de otro tipo. Le voy a decir brevemente lo que estamos haciendo en la IETF respecto de esto. Siempre estamos preocupados por la seguridad, por supuesto, y en varios aspectos. Por ejemplo, hemos tenido muchas peleas en las últimas dos décadas sobre si debíamos permitir la encripción en la Red. Afortunadamente, se decidió que sí. Sin esa decisión, el e-commerce no podría existir. Además, tenemos las revelaciones de que hay mucha más vigilancia que la pensábamos, y más extendida, y en la IETF, luego de mucho debate, decidimos que la vigilancia masiva es una amenaza para las comunicaciones en Internet. Y decidimos eso porque si los protocolos tienen alguna debilidad que una agencia de seguridad puede explotar, entonces mañana podrán hacerlo los criminales. Así que no podemos realmente dejar ninguna vulnerabilidad. Estamos intentando eliminar esas debilidades. Estamos trabajando en los algoritmos que operan debajo de HTTPS (https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure) y TLS (https://es.wikipedia.org/wiki/Transport_Layer_Security), y en una nueva versión

de TLS. HTTP/2 es más rápido, pero también es más eficiente en términos de seguridad. Es decir, la seguridad de la conexión no va a impactar en la performance de la conexión, como ocurría antes. Y hemos creado nuevos grupos de trabajo, luego de las revelaciones de Snowden, específicamente para abordar el tema de la privacidad.

-Ustedes publicaron un documento (https://tools.ietf.org/html/rfc7258) donde dicen específicamente que la vigilancia generalizada equivale a un ataque. Eso es fuerte. ¿Por qué ponen a la misma altura la vigilancia de una agencia de inteligencia y un ataque a la Red?

B. L.: -Si no podés distinguir a alguien que está haciendo vigilancia y es considerado de los buenos del que está interceptando datos en la Red y es un criminal, si los protocolos pueden ser intervenidos, entonces se trata de un ataque al sistema. No es una afirmación política. Sólo decimos que si hay una vulnerabilidad, tenemos que arreglarla.

-Se supone, sin embargo, que por eso es vigilancia, porque no se la puede detectar. ¿Es una vulnerabilidad o es un ataque?

B. L.: -Interceptar datos privados es un ataque.

-Pero esa es la misión de la NSA (www.nsa.gov), por citar una agencia.

J. A.: -Sí, así es. Nosotros no estamos haciendo una declaración política ni un juicio de valor. Estamos haciendo una afirmación técnica. Si hay un protocolo que tiene una debilidad que permite monitorear la comunicación, entonces hay un problema.

-¿Es un problema con el monitoreo o con el protocolo?

B. L.: -Es un problema con el protocolo. Nosotros no estamos diciendo si la NSA o las otras agencias de seguridad tenían el derecho de efectuar ese monitoreo, ni si eso está bien o mal. Lo que decimos es que si un protocolo permite ese monitoreo, entonces no es seguro y debemos cambiar eso.

-Me encanta ver que la IETF equipara el monitoreo generalizado con un ataque a las comunicaciones, pero, ¿es posible blindar los protocolos y la infraestructura de red de tal modo que ni siquiera una agencia con los

enormes recursos de la NSA pueda realizar ese monitoreo?

J. A.: -Sí y no. No creemos tener el conocimiento perfecto, pero las recomendaciones de todo mundo en la comunidad criptográfica dicen que las herramientas de encriptado fuertes y los protocolos criptográficos siguen siendo nuestra mejor apuesta y que van a asegurarnos contra ataques, supuesto el caso de que usemos los algoritmos correctos. Así que creo que es posible protegernos, si somos cuidadosos y diseñamos nuestra tecnología adecuadamente. Pero esa es solamente la parte que concierne a la seguridad de las telecomunicaciones, porque si te comunicás con alguien en quien no confiás por completo, esa persona puede ser inducida por el gobierno a entregar tus datos.

-Mi sensación es que nunca vamos a sentirnos seguros, luego de las revelaciones de Snowden.

J. A.: -Y nunca vamos a tener una seguridad perfecta. Lo mejor que podemos hacer es aplicar las mejores tecnologías que conocemos. Eso significa que es lo mejor que podemos hacer, no lo mejor posible. No equivale a decir que nadie va a quebrantar esa seguridad, sino que es lo mejor que sabemos hacer.

-Mientras tanto más de 1000 millones de personas están subiendo a Facebook casi cada pequeño detalle de sus vidas privadas.

B. L.: -Y lo hacen de forma voluntaria y completamente insegura.

J. A.: -Herramientas de encriptación muy populares, como PGP (https://es.wikipedia.org/wiki/Pretty_Good_Privacy) han recorrido un largo camino, pero siguen siendo vulnerables a cosas como: "¿Usted confía en su computadora?"

-Muchas personas creen, y eso me incluye, que Internet nació como un desarrollo militar, dadas las circunstancias en que fue creada. Es decir, que Arpanet tenía originalmente la meta de proveerle a Estados Unidos un mecanismo de comunicación que pudiera resistir un ataque nuclear. Estados Unidos hoy lo niega. ¿Cuál es la verdad?

B. L.: -Ni Jari ni yo estábamos en esto por entonces, pero ARPA [hoy DARPA; http://www.darpa.mil] es una agencia del gobierno que forma parte del Departamento de Defensa. Sus proyectos fueron solventados por los militares,

pero la mayoría de los desarrollos los hicieron las universidades. Creo que Estados Unidos es sincero cuando dice que no creó Arpanet como un sistema militar, pero lo desarrollaron con fondos militares, así que existía por lo menos la idea de un sistema de comunicaciones para casos de desastres, si no acaso algo más.

J. A.: -Pienso que es una perspectiva interesante, pero a la larga no importa, porque lo que tenemos es una tecnología de propósito general que es flexible y esa es la razón por la que ha sido tan enormemente exitosa.

B. L.: -Creo que lo que pasó no afecta a Internet hoy.

-Si es verdad, hemos transformado un proyecto militar en la tecnología más democratizadora desde Gutenberg para acá, y una forma disruptiva de comunicaciones para 3000 millones de personas. No lo hicimos tan mal.

B. L.: -Es especialmente interesante porque le ha cambiado la vida a millones de personas, para bien.

-Usted habló de la IoT hace unos minutos, y es algo interesante y en gran medida inevitable. Vamos hacia un mundo en el que todo está interconectado (incluso su lavarropas). ¿Pero cuáles son los desafíos?

J. A.: -Hay múltiples problemas. Hay un problema de seguridad generalizado. Y hay un problema de privacidad. Es decir, cuánta información distribuimos, y esto en muchos niveles. Y hay también un problema de mantenimiento. Cuántos dispositivos hay, dónde están, cuáles son sus direcciones y demás. Tiene que haber una manera más inteligente de administrar y mantener todo eso que a mano. Así que hay problemas, sí, mucho trabajo por hacer.

-Sé que a nadie le gusta arriesgar predicciones, ¿pero qué cambios prevén para dentro de 10 o 15 años?

B. L.: -Bueno, hay cosas que son fáciles de predecir, como que el número de dispositivos conectados va a crecer y que tenemos que hacer algo con eso. Pero dentro de 10 o 20 años podría darse un cambio más radical en la naturaleza de las cosas. Por ejemplo, usted piensa en su auto como algo que posee. Quizás en el futuro eso ya no sea así, quizá los coches sean un servicio que usted compra. Y como todo va a estar conectado, el auto va a ir a cargar nafta por las suyas

cuando lo necesite. Para muchos de nosotros va a ser algo extraño, porque tenemos la mente modelada de otra forma y vemos los autos como posesiones. Pero para los más jóvenes eso va a ser lo natural. Incluso el concepto mismo de muchos negocios va a cambiar, creo que ese va a ser algo que viene.

-Díganme algo que les haya llamado la atención de Buenos Aires.

B. L.: -Este es mi primer viaje a Buenos Aires y por ahora me lo he pasado de reunión en reunión, no he visto mucho.

J. A.: -Es una ciudad encantadora, empezando por el hecho de que vuestros inviernos son más cálidos que nuestros veranos.

lanacion.com | Tecnología