Seguridad de enrutamiento para legisladores:
un documento técnico de Internet Society

Octubre 2018

Aunque el usuario promedio no lo puede ver, el enrutamiento del Protocolo Internet (IP) es el apoyo de Internet. Al asegurar que los paquetes[1] vayan a donde se supone que deben hacerlo, el enrutamiento[2] desempeña un rol central en la función confiable de Internet. Se asegura de que los correos electrónicos lleguen a los destinatarios correctos, que los sitios de comercio electrónico sigan operando y que los servicios de gobierno electrónicos sigan atendiendo ciudadanos. La seguridad del sistema de enrutamiento global es imprescindible para el crecimiento continuo de Internet y para salvaguardar las oportunidades que proporciona a todos los usuarios.

Cada año ocurren miles de incidentes de enrutamiento[3], cada uno con el potencial de dañar la confianza del usuario e incapacitar el potencial de Internet.[4]Estos incidentes de enrutamiento pueden crear también daños económicos reales. Los servicios clave se vuelven inaccesibles, perturbando la habilidad de las empresas y de los usuarios de participar en el comercio electrónico.[5]O pueden desviarse paquetes a través de redes maliciosas, lo que brinda una oportunidad de espiar sus datos.[6]Si bien las medidas de seguridad conocidas pueden lidiar con muchos de estos incidentes de enrutamiento, las incentivas desalineadas limitan su uso.

Todos los actores, incluyendo los legisladores, deben adoptar medidas para fortalecer la seguridad del sistema de enrutamiento global.[7]Esto solo puede hacerse si se preservan al mismo tiempo los aspectos vitales del sistema de enrutamiento que han permitido que Internet sea una red tan ubicua y se

---

1Los paquetes de red, o "paquetes", son datos que se envían a través de una red o redes.

2El enrutamiento es la práctica de determinar la forma de obtener datos de una ubicación a otra, a través de una red o de varias redes.

3Los incidentes de enrutamiento son actualizaciones al Protocolo de puerta de enlace de frontera (Border Gateway Protocol) que tienen un impacto negativo.

4https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

5Por ejemplo, en abril de 2017, una fuga de rutas provocó una "perturbación en Internet a gran escala que ralentizó o bloqueó el acceso a los sitios Web y servicios en línea para docenas de empresas japonesas".https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

6Durante varios minutos en abril de 2017, un operador de red secuestró sospechosamente el tráfico de Internet de varios servicios financieros. Si es intencional, el secuestro podría usarse para permitir que el operador de red lea información financiera sin encriptar a medida que pase por sus redes, o tratar de descifrar la información financiera encriptada.https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

7Si bien otras formas de seguridad (seguridad física o seguridad de los datos) son importantes para todos los actores, incluidos los operadores de redes, este documento normativo busca enfocarse únicamente en mejorar la seguridad del enrutamiento. Si desea más información sobre proteger la infraestructura de los proveedores de servicios de Internet, vea: https://www.rfc-editor.org/rfc/rfc3871.txt

mejora su seguridad. Predicando con el ejemplo en sus propias redes, fortaleciendo la comunicación y ayudando a realinear incentivos para favorecer una seguridad más sólida, los legisladores pueden ayudar a mejorar el ecosistema de seguridad del enrutamiento.

Consideraciones clave

En esencia, el sistema de enrutamiento se basa en la confianza entre redes. El sistema de enrutamiento global es un sistema complejo y descentralizado, conformado por decenas de miles de redes individuales. Las decisiones de negocios independientes y las relaciones de confianza entre operadores de redes individuales que implementan el Protocolo de puerta de enlace de frontera (Border Gateway Protocol o BGP en inglés) determinan la forma en que opera la red.[8]La arquitectura del sistema mallado contribuye a su resiliencia, escalabildidad y facilidad de adopción.

Ya que no tiene un solo punto de falla o un controlador individual, el sistema de enrutamiento es difícil de infringir a nivel global, fácil de conectar y puede escalar sin problemas. Cuando una ruta se congestiona o falla, las redes pueden optar por enrutar el tráfico alrededor de las áreas problemáticas. La estructura del sistema de enrutamiento también permite una excelente cantidad de flexibilidad para que los operadores de red gestionen sus propias redes. Esto permite a los operadores de red desarrollar arquitecturas y soluciones de red novedosas que se adapten de la mejor manera a las necesidades de sus usuarios. Estas cualidades han hecho que Internet tenga tanto éxito además de permitir su crecimiento.

Desafíos

Si bien las cualidades del sistema de enrutamiento han permitido su éxito en general, estos mismos atributos pueden contribuir también a algunos de sus desafíos. El sistema está basado en cadenas de confianza; cada red depende de sus redes vecinas (que a su vez dependen de sus propias vecinas, etc.) para actuar en forma apropiada. No hay verificación integrada y es fácil tergiversar la información. Esto conduce a **incidentes de enrutamiento** continuos. Las complejidades y la descentralización del sistema de enrutamiento global también generan **desafíos en el ecosistema**, incluyendo incentivos desalineados y los riesgos externalizados que plantea la inseguridad del enrutamiento. Se conocen las soluciones para lidiar con muchos incidentes de enrutamiento, pero los desafíos del ecosistema dificultan su implementación. Cualquier esfuerzo por lidiar con estos desafíos debe reconocer las funciones técnicas básicas del sistema de enrutamiento y mantener los beneficios que proporciona la arquitectura del sistema de enrutamiento.

En 2017 hubo cerca de 14,000 incidentes de enrutamiento registrados en total.[9]Los incidentes afectaron a más del 10% de los sistemas autónomos (AS) en Internet. Hay tres tipos principales de incidentes de enrutamiento:

- **Apropiación de ruta/prefijo,** en donde un operador de red o atacante se hace pasar por otro operador de red, pretendiendo que es la ruta correcta al servidor o red que se busca en Internet.[10]

8Un *protocolo de enrutamiento* es la forma en que una red determina la ruta que va a tomar un paquete de datos. Para enrutar el tráfico entre redes, la mayoría de las redes usan el Protocolo de puerta de enlace de frontera (Border Gateway Protocol, o BGP).

9https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

10En un secuestro de ruta, un operador de red o atacante se hace pasar por otro operador de red, pretendiendo que es la ruta correcta al servidor o red que se busca en Internet. Esto puede provocar que se reenvíen paquetes al lugar incorrecto, ataques de negación de servicio (DoS) o intercepción de tráfico.

- **Fugas de ruta,** son la propagación de anuncios de enrutamiento[11] más allá de su alcance previsto (infringiendo sus políticas).[12,13]

- **Falsificación de IP,** en donde alguien crea paquetes IP con una dirección IP de origen falsa para ocultar la identidad del remitente o hacerse pasar por otro sistema.[14]

Esos incidentes pueden ejercer mucha presión sobre la infraestructura y provocar caída de tráfico, proveer los medios para la inspección de tráfico o incluso usarse para realizar ataques de amplificación de servidores de nombres de dominio (DNS)[15] o cualquier otro ataque de amplificación reflectiva (RA).[16]

Las prácticas recomendadas en la seguridad del enrutamiento ya están disponibles y se consideran muy efectivas en contra de estas formas de incidentes de enrutamiento. Tanto para las fugas de rutas como para las apropiaciones de ruta, los operadores de red pueden usar políticas de filtrado más sólidas[17] y determinar cuándo es que las redes vecinas hacen anuncios perjudiciales. La validación de origen de una dirección IP[18] puede usarse para encontrar tráfico falsificado a medida que entra o sale de una red. Después el tráfico falsificado puede filtrarse para evitar que llegue a su destino. Hay esfuerzos continuos por desarrollar herramientas aún más efectivas como la Validación del origen de la ruta (Route Origin Validation, o ROV)[19] y fortalecer las existentes, como definir con más detalle una 'ruta viable' en la tecnología Unicast Reverse Path Forwarding (uRPF).[20]

Las **Normas mutuamente acordadas para la seguridad del enrutamiento (Mutually Agreed Norms for Routing Security, o MANRS)[21]** son un conjunto de prácticas de referencia visibles para que los operadores de red mejoren la seguridad del sistema de enrutamiento global. En 2014, un grupo de operadores de redes con ideas afines desarrolló MANRS como una iniciativa voluntaria. Define cuatro acciones simples pero concretas que los operadores de redes pueden implementar para mejorar de manera considerable la seguridad y confiabilidad de Internet.[22]Las primeras dos mejoras (filtrado y validación de origen de IP) tratan con las causas raíz de los incidentes de enrutamiento comunes. Las

11Las redes se hacen *anuncios* entre sí, en donde se detallan las direcciones accesibles mediante su red o dentro de la misma, o de las redes de un cliente. Los anuncios ayudan a determinar cómo deciden los enrutadores canalizar el tráfico hacia un destino. Las *políticas de anuncios* determinan lo que una red anunciará a un vecino.

12https://tools.ietf.org/html/rfc7908#section-2

13Por ejemplo, un operador de red con más de un proveedor inmediato (upstream) anuncia a un proveedor inmediato que tiene una ruta hacia un destino a través del otro proveedor inmediato (a menudo debido a una configuración irregular accidental).O una red grande podría anunciar de manera no intencional rutas a todas sus redes descendentes (downstream).Si es maliciosa, una fuga de ruta puede usarse para inspección y reconocimiento de tráfico o (a menudo cuando es accidental) puede presionar gravemente la infraestructura.

14En la falsificación de IP, alguien crea paquetes IP con una dirección IP de origen falsa para ocultar la identidad del remitente o hacerse pasar por otro sistema. La falsificación de IP puede usarse para realizar ataques de amplificación en servidores de nombres de dominio (DNS)

15Un ataque de amplificación en un DNS se ejecuta enviando muchas solicitudes a muchos resolvedores de DNS mientras se falsifica la dirección IP de la víctima; un atacante puede pedir muchas respuestas a los resolvedores de DNS para regresar a un destino aunque solo utilice un sistema para realizar dicho ataque.

16https://www.us-cert.gov/ncas/alerts/TA14-017A

17Cada red determina lo que puede aceptar como anuncio de otras redes, esta es su *"política de filtrado".*

18La validación de origen de dirección IP consiste en técnicas que se utilizan para asegurar que la dirección IP proporcionada por un paquete provenga de una dirección de origen válida.

19https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800-14-draft.pdf

20https://tools.ietf.org/html/draft-sriram-opsec-urpf-improvements-03

21https://www.manrs.org/

22https://www.manrs.org/manrs/

otras dos (coordinación[23] y validación global[24]) ayudan a limitar el impacto de los incidentes y reducen la probabilidad de estos en el futuro.

Cada una de las acciones de MANRS prescribe resultados en vez de métodos específicos. Esto permite que la implementación cambie con la tecnología. Además de los incidentes de enrutamiento, MANRS busca lidiar con los desafíos del ecosistema en el sistema de enrutamiento global. MANRS mejora los incentivos económicos de la seguridad del enrutamiento al permitir que los operadores de redes indiquen su postura de seguridad de enrutamiento a los clientes, competidores y legisladores. Además proporciona las métricas para medir la seguridad del enrutamiento. Las mediciones de MANRS pueden servir como u9na valiosa evaluación de un tercero en cuanto a las prácticas de seguridad de un operador de red.[25]

A pesar de la disponibilidad de soluciones a los incidentes de enrutamiento comunes, los desafíos del ecosistema limitan su uso.

- **Los incidentes de enrutamiento son difíciles de resolver lejos del origen, por lo que mejor deben tratar de solucionarse colectivamente.** De cualquier parte de donde provenga una amenaza, las redes cerca de su origen están en la mejor posición para lidiar con dicha amenaza (por ejemplo, las redes adyacentes pueden rehusarse a aceptar anuncios falsos).[26]Cuando una red se ve afectada más allá del origen de un incidente de enrutamiento, solo puede tratar de mitigar el impacto. Debe depender de otras redes más cerca del problema del incidente de enrutamiento para lidiar con el problema por completo.

- **Factores externos económicos.** Cualquier red puede ser el origen de un incidente y la inseguridad de una red puede afectar a todas las demás. Ahora bien, incluso si un incidente de enrutamiento se origina desde nuestra propia red, es muy probable que el impacto se sienta en otra red. Es menos probable que los operadores de red inviertan recursos en mejorar la seguridad del enrutamiento, ya que los beneficios serán en su mayoría para otras redes y no las suyas.

- **La seguridad del enrutamiento no es un diferenciador del mercado.** Actualmente, una buena seguridad de enrutamiento no es una herramienta de marketing efectiva para los operadores de redes. Es difícil que los operadores de redes comuniquen su nivel de seguridad de enrutamiento a sus clientes. Los usuarios tienen una comprensión limitada en cuanto al sistema de enrutamiento global y la forma en que las prácticas de seguridad de enrutamiento de su red puede impactar.

23Como los incidentes de enrutamiento se resuelven mejor cerca de su origen, son imprescindibles las acciones para mejorar la coordinación entre operadores de redes (que puede ser tan simple como tener la información de contacto disponible al público y actualizada).

24Al documentar públicamente su política de enrutamiento y lo que pretenden anunciar a las partes externas, otros pueden validar sus anuncios.

25Hay un portal en línea para ver estas métricas, se llama The MANRS Observatory, está en desarrollo y se espera que esté listo a finales de 2018.

26"En la política, a dicha metodología se le conoce como principio de subsidiariedad: las soluciones deben definirse e implementarse mediante una autoridad competente más pequeña, inferior o menos centralizada".https://www.internetsociety.org/collaborativesecurity/approach/#_ftnref5

Recomendaciones y principios fundamentales

La acción colectiva global es la única forma de lidiar con las amenazas de seguridad del enrutamiento y fortalecen dicha seguridad. Todos los actores, incluidos los gobiernos, desempeñan roles importantes para mejorar los incentivos del mercado y fortalecer la seguridad del enrutamiento, impulsar el desarrollo o la adopción de prácticas recomendadas y eliminar barreras además de fortalecer la cooperación. Sin embargo, cualquier acción debe elaborarse cuidadosamente para no limitar las ventajas del sistema de enrutamiento global, incluyendo su resiliencia en general, facilidad de uso, flexibilidad y escalabilidad. Para mejorar la seguridad del enrutamiento debemos:

- **Liderar con el ejemplo.** Todos los actores, incluidos los gobiernos, deben mejorar la confiabilidad y seguridad de la infraestructura mediante la adopción de las prácticas recomendadas en sus propias redes.
    - Todas las redes que proporcionen conectividad a Internet, incluyendo las redes empresariales o gubernamentales, deben usar filtrado además de la validación del origen de direcciones IP para ayudar a prevenir y mitigar el impacto de los incidentes.
    - Además, los participantes influyentes del mercado, como las grandes empresas o gobiernos, deben, cuando sea posible, exigir el cumplimiento con las referencias de seguridad del enrutamiento, como la que está documentada por MANRS, para la adquisición de contratos con proveedores de servicios de Internet. MANRS, a través de su MANRS Observatory, proveerá mediciones que pueden servir como la valiosa evaluación de un tercero en cuanto a las prácticas de seguridad de un operador de red. Estas evaluaciones pueden ayudar a informar las decisiones de adquisición.
- **Facilitar/fomentar la adopción de prácticas comunes para la seguridad del enrutamiento.** Las asociaciones de la industria, en estrecha colaboración con los gobiernos y demás actores, deben promover una referencia común para la seguridad del enrutamiento.
    - La referencia común para los operadores de redes provee un estándar industrial para la seguridad del enrutamiento y promueve un mayor intercambio de información entre operadores de redes. También provee un método para que los operadores de redes indiquen su nivel de seguridad a los posibles clientes.
    - Todos los actores pueden contribuir a la adopción y el desarrollo de prácticas comunes de referencia y de la industria para la seguridad del enrutamiento, al participar en el proceso de desarrollo y, cuando sea viable, por medio del financiamiento.
- **Apoyar los esfuerzos para desarrollar nuevas herramientas de seguridad del enrutamiento o fortalecer las existentes.** El hecho de mejorar aún más la seguridad de las sociedades de sistemas de enrutamiento globales con la comunidad de investigación podría ayudar a desarrollar la próxima generación de herramientas y prácticas de seguridad del enrutamiento.
    - En donde sea posible, los actores, incluidos los gobiernos y el sector privado, pueden incrementar el financiamiento para la investigación, el desarrollo y el despliegue experimental de la próxima generación de protocolos de Internet, incluidos los que mejoran la seguridad del enrutamiento.

  - Los investigadores pueden desarrollar asesoría técnica en cuanto a realizar una validación del origen de direcciones IP, un filtrado efectivo y una validación global. La asesoría también debe animar a los operadores de redes a implementar BGPSec[27] y RPKI.[28]

- **Fomentar el uso de la seguridad como un diferenciador competitivo.** Para que la seguridad del enrutamiento sea un diferenciador competitivo, los actores deben respaldar el conocimiento público sobre la importancia de la seguridad del enrutamiento y fomentar una mayor señalización de la seguridad del enrutamiento entre la industria y los clientes.

  - Para los proveedores de servicios de Internet, la seguridad del enrutamiento es un componente básico de su postura de seguridad en general. La señalización de su postura hacia la seguridad del enrutamiento se refleja de manera considerable en su postura general, lo que puede diferenciar sus servicios de los de la competencia.

  - Las empresas pagarán más por una mejor seguridad en el enrutamiento, pero necesitan formas de diferenciar la buena seguridad del enrutamiento de la mala. En una encuesta de 2017, el 94% de las empresas indicaron que estarían dispuestas a pagar más por un distribuidor que fuera miembro de MANRS en una situación competitiva.[29]La misma investigación encontró además que el conocimiento sobre MANRS era marginal entre las empresas antes de la encuesta.

  - La industria, los grupos de consumidores, gobiernos y otros actores deberían trabajar en conjunto para promover el uso de referencias de seguridad del enrutamiento, tales como MANRS, como un diferenciador competitivo.[30]Además deberían apoyar los esfuerzos por educar a las empresas locales en cuanto a la seguridad del enrutamiento y las prácticas recomendadas existentes.

- **Fortalecer la comunicación y cooperación entre los operadores de redes y otros actores.** Los actores deben respaldar el desarrollo de mejores mecanismos para compartir información, participar en el intercambio de información sobre la seguridad del enrutamiento y colaborar con actores para resolver las amenazas de seguridad del enrutamiento.

  - El sector privado, los gobiernos, la sociedad civil, el ámbito académico y otros pueden respaldar el desarrollo de equipos de respuesta a incidentes de seguridad computacional (CSIRT) o fortalecer los ya existentes. Los CSIRT desempeñan un rol importante en el intercambio de información y la coordinación en respuesta a los incidentes y amenazas del enrutamiento.

- **Identificar y resolver las barreras legales para el intercambio de información, la implementación de tecnologías de seguridad del enrutamiento y la investigación tanto de**

27BGPSec es una extensión del Protocolo de puerta de enlace de frontera (Border Gateway Protocol, o BGP), el cual provee seguridad para la ruta de sistemas autónomos (AS) a través de los cuales pasa un mensaje de actualización de BGP.https://tools.ietf.org/html/rfc8205

28"Con RPKI, la Infraestructura de claves públicas de recursos (Resource Public Key Infrastructure), los anuncios de ruta del Protocolo de puerta de enlace de frontera (BGP) que se emiten desde un enrutador se validan para asegurar que la ruta provenga del que posee los recursos y que sea una ruta valida."https://www.arin.net/resources/rpki/

29Informe de estudio del proyecto MANRS. Investigación 451.https://www.routingmanifesto.org/wp-content/uploads/sites/14/2017/10/MANRS-451-Study-Report.pdf

30MANRS, un conjunto visible de prácticas recomendadas y a través de sus mediciones públicas que se proporcionan a través del MANRS Observatory, tiene el potencial de ser una herramienta de marketing poderosa para los proveedores de servicios de Internet.

incidentes como de amenazas de enrutamiento. Las barreras legales pueden impedir que los investigadores de seguridad y desincentivar a los operadores de redes para que no implementen soluciones de seguridad del enrutamiento ni compartan información entre sí.

- Identificar y eliminar las barreras legales y regulatorias puede mejorar el intercambio de información y las respuestas a los incidentes de enrutamiento. A los actores, en especial los investigadores de seguridad, les puede preocupar que divulgar los incidentes o amenazas de seguridad del enrutamiento pueda traerles un problema legal. Las barreras legales pueden impedir también el desarrollo y despliegue de las tecnologías de seguridad del enrutamiento. Al desarrollar soluciones a las barreras identificadas, los actores deben poner mucha atención en su impacto potencial sobre la privacidad de los individuos.

Conclusión

El sistema de enrutamiento global es increíblemente resistente. Su estructura descentralizada proporciona flexibilidad, escalabilidad y resistencia en general. Aunque su estructura ha desempeñado un rol crucial en el crecimiento de Internet, también ha permitido que ocurran incidentes en el enrutamiento.

Las mejores prácticas, como las Normas mutuamente acordadas para la seguridad del enrutamiento, proporcionan una ruta clara que los operadores de redes pueden adoptar para resolver estas amenazas de enrutamiento. Sin embargo, todos los actores necesitan adoptar medidas para lidiar con los desafíos del ecosistema que evitan la aplicación generalizada de las prácticas recomendadas. Solo a través de la acción colectiva podemos resolver los desafíos de seguridad de enrutamiento y mantener al mismo tiempo los beneficios de un sistema de enrutamiento descentralizado.