Análisis Técnico de la Infraestructura de Clave Pública de Recursos (RPKI)

Oficina del Director de Tecnologías de la ICANN

Alain Durand
OCTO-014
2 de septiembre de 2020

ICANN

ÍNDICE

El presente documento es parte de la serie de documentos de la OCTO. Consulte la página de publicaciones de la OCTO para ver la lista de documentos de la serie. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, las puede enviar a octo@icann.org.

Resumen Ejecutivo

El Protocolo de Frontera de Entrada (BGP) es el protocolo de enrutamiento utilizado en línea por los proveedores de servicios de Internet (ISP). Existe desde comienzos de la década de 1990. Los incidentes de enrutamiento de BGP, como la ampliamente divulgada fuga de ruta de YouTube por parte de Pakistan Telecom en 2008, se conocen como fugas de rutas y pueden crear desvíos de tráfico en toda Internet. Ahora ocurren a diario y suponen un perjuicio muy grande para las operaciones de los ISP. Estos desvíos pueden ser el resultado de errores de configuración, fallas de software o ataques activos. La raíz de estos problemas es la falta de seguridad incorporada en el protocolo BGP.

El fortalecimiento de la seguridad es una iniciativa compleja y prolongada que aún no ha concluido. Dentro de las opciones disponibles en la actualidad, la más avanzada es la validación de origen con RPKI. La validación de origen con RPKI utiliza la Infraestructura de Clave Pública de Recursos (Resource PKI, o RPKI), un marco jerárquico de certificados de clave pública X.509 entrelazados que están anclados en los Registros Regionales de Internet (RIR). Su objetivo es validar que los ISP que originan rutas de Internet estén autorizados a hacerlo por el titular de los correspondientes bloques de direcciones del Protocolo de Internet (IP). La validación de origen con RPKI existe desde 2011. Ahora está cobrando impulso como resultado de diversos factores, tales como las iniciativas lideradas por los RIR durante muchos años para promover esta solución y capacitar a los profesionales de la ingeniería en su uso, las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS) de la Internet Society y la financiación del Departamento de Seguridad Nacional de Estados Unidos para el desarrollo de software de RPKI. Este contexto, sumado a la creciente impaciencia por las fugas en las rutas que llevan a la sensación de que "hay que hacer algo", además de los ejemplos establecidos por algunos grandes proveedores (como Cloudflare y NTT), hizo que la validación de origen con RPKI sea un tema candente en 2020.

Aun así, la tecnología es inmadura. Existen graves problemas de escala que dan lugar a demoras de propagación que reducen la flexibilidad de los ISP para hacer frente a las emergencias y suponen una fragilidad para el sistema. El propio sistema RPKI puede ser atacado. Podría ser difícil detectar un escenario de falla catastrófica e incluso más difícil recuperarse de tal escenario. Esos riesgos se ven agravados por el modelo de despliegue que utiliza cinco anclajes de confianza, lo que abre la posibilidad de que haya incoherencias en los datos y allana el camino para una cantidad aún mayor de anclajes de confianza. Las partes que no utilizan en absoluto la RPKI también pueden convertirse en víctimas colaterales de un incidente en cualquiera de los anclajes de confianza. El Registro Norteamericano de Números de Internet (ARIN) considera que los riesgos de responsabilidad civil derivados de esos escenarios son tan elevados que el RIR exige una indemnización a las partes dependientes por el uso de sus datos de RPKI. El sistema hizo que los RIR sean participantes activos del funcionamiento cotidiano de Internet, un rol para el que pueden o no ser los más adecuados, como lo demuestran algunos incidentes recientes.

Hay un factor incluso más importante: al limitar el alcance al origen de los anuncios de ruta, la validación de origen con RPKI solo protege de los ataques más ingenuos al sistema de enrutamiento. Un sistema de seguridad de enrutamiento sólido requiere una validación completa de la ruta, pero eso es significativamente más complejo.

Varios proveedores de servicios de Internet, puntos de intercambio de Internet (IXP) y proveedores de servicios en la nube consideran que detener las fugas en las rutas derivadas de errores de configuración y errores de software mediante la validación de origen con RPKI es una mejora operativa que justifica el costo de desplegar este sistema bastante complejo. Aun así, quien contemple la posibilidad de desplegar la validación de origen con RPKI debería ser consciente del grado actual de madurez de esta solución y los riesgos operativos que conlleva. Asegurar la infraestructura de enrutamiento no es (todavía) una cuestión tan sencilla como implementar un programa informático. El equilibrio entre la seguridad de los protocolos y la complejidad operativa debe ponderarse con cautela.

Consulte la Publicación 014 de la OCTO para acceder al documento completo (en inglés).

Conclusión

Existe un gran interés en la RPKI por parte de los RIR y los operadores de redes, tanto grandes como pequeños. Para una gran cantidad de actores, la RPKI ofrece beneficios suficientes como para lograr un retorno positivo de la inversión. La firma de las Autorizaciones de Origen de Ruta (ROA) ahora es lo suficientemente simple como para que prácticamente cualquier titular de una dirección IP pueda hacerla, y la validación de origen con RPKI ofrece protección contra la digitación inexacta, los errores de configuración y los errores de software. Aunque la validación de origen con RPKI no protege al sistema de enrutamiento de los ataques intencionales, desde la perspectiva de los operadores, tanto los ataques al sistema de enrutamiento como las fugas de ruta derivadas de la digitación inexacta generan tickets que deben resolverse. Cualquier ayuda que la validación de origen con RPKI proporcione en ese frente será definitivamente bienvenida por una gran cantidad de ISP.

Sin embargo, el sistema general, basado en los certificados X.509, es complejo. Esta complejidad introduce el riesgo de que nuevos errores, errores tipográficos e instancias de digitación inexacta terminen en la propia RPKI. Una sólida experiencia organizacional en la gestión de sistemas criptográficos probablemente seguirá siendo un requisito previo para activar la validación de origen de ruta (ROV). La RPKI en sí misma tiene algunos inconvenientes. El retraso en la propagación, que puede llegar a ser de hasta 24 horas, agravado por la falta de monitoreo sistemático generalizado, puede ser un problema operativo importante. También cabe señalar que, además de no abordar todos los aspectos del problema de la seguridad de enrutamiento, la validación de origen con RPKI puede introducir nuevas amenazas en el sistema de enrutamiento, como en el caso de los ataques a los repositorios de RPKI, los diversos certificados o los sistemas de distribución de las ROA. Hasta la fecha, la ROV para validación de origen con RPKI solo se ha desplegado a escala limitada. Todavía hay preguntas por responder con respecto a la escalabilidad del sistema en general.

En última instancia, serán los operadores de redes quienes tengan que determinar si el costo de esta infraestructura bastante específica y la complejidad operativa de la validación de origen con RPKI se justifican en pos del beneficio en términos de integridad de enrutamiento. Algunos operadores de redes, preocupados por el impacto en sus operaciones de las fugas de rutas inducidas por una mala configuración, creen claramente que este es el caso; otros operadores, preocupados por la seguridad de enrutamiento, aún no se han convencido. Tal vez lo más importante es que la RPKI implica ciertos cambios en las estructuras operativas críticas de Internet en su conjunto. Todavía no está claro si las comunidades afectadas e impactadas por

esos cambios son plenamente conscientes de esas implicancias. Claramente, es necesario continuar trabajando para comunicar las implicancias de la RPKI.

Agradecimientos

Si bien todas las opiniones que figuran en este informe son las del autor, quisiéramos agradecer a las siguientes personas por sus aportes, comentarios o revisiones durante la elaboración del informe:

- Alain Aina, WACREN
- Rob Austein, Hacntr
- John Curran, ARIN
- Kim Davies, ICANN (IANA)
- Geoff Huston, APNIC
- Fredrik Korsback, Amazon
- Nathalie Künnake-Trenaman, RIPE NCC
- Martin Levy, Cloudflare
- Di Ma, ZDNS
- Terry Manderson, ICANN (Ingeniería de Redes y del DNS)
- Carlos Martinez, LACNIC
- Christopher Morrow, Google
- Ricardo Patara, NIC Brasil
- Amreesh Phokeer, AFRINIC
- Andrei Robachevsky, ISOC
- Job Snijders, NTT
- Bill Woodcock, PCH

Un especial agradecimiento a David Huberman (ICANN) por su constante apoyo y disposición a escuchar consultas mientras redactaba este documento.