RPKI: Validación de Origen en BGP

Guillermo Cicileo
guillermo@lacnic.net

lacnic32
lacnog 2019
7–11 OCTUBRE / CIUDAD DE PANAMÁ, PANAMÁ

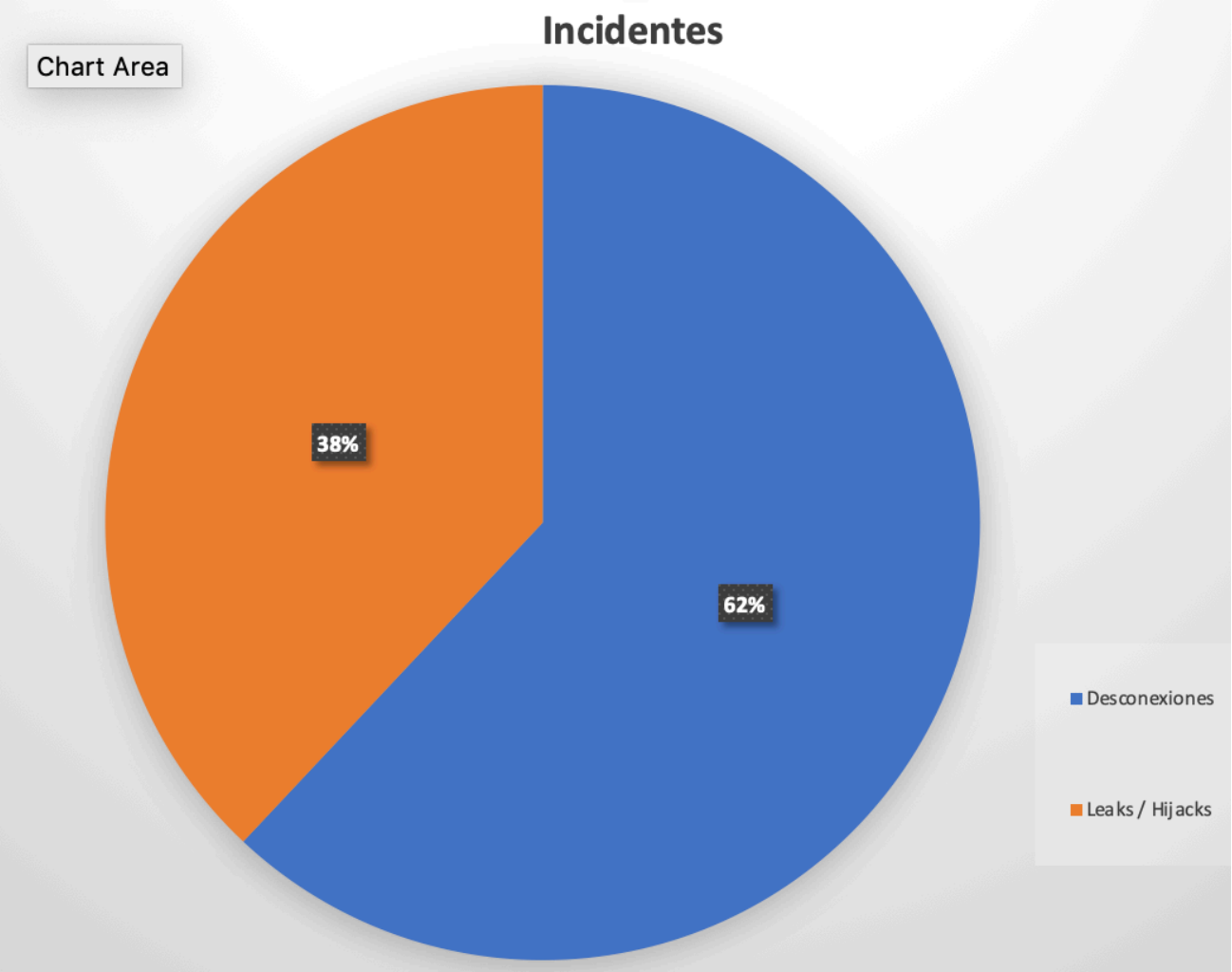
12.600 incidentes de ruteo en 2018

Alrededor de 4.5% de todos los sistemas autónomos de Internet fueron afectados

2,737 sistemas autónomos fueron víctimas de algún incidente de ruteo

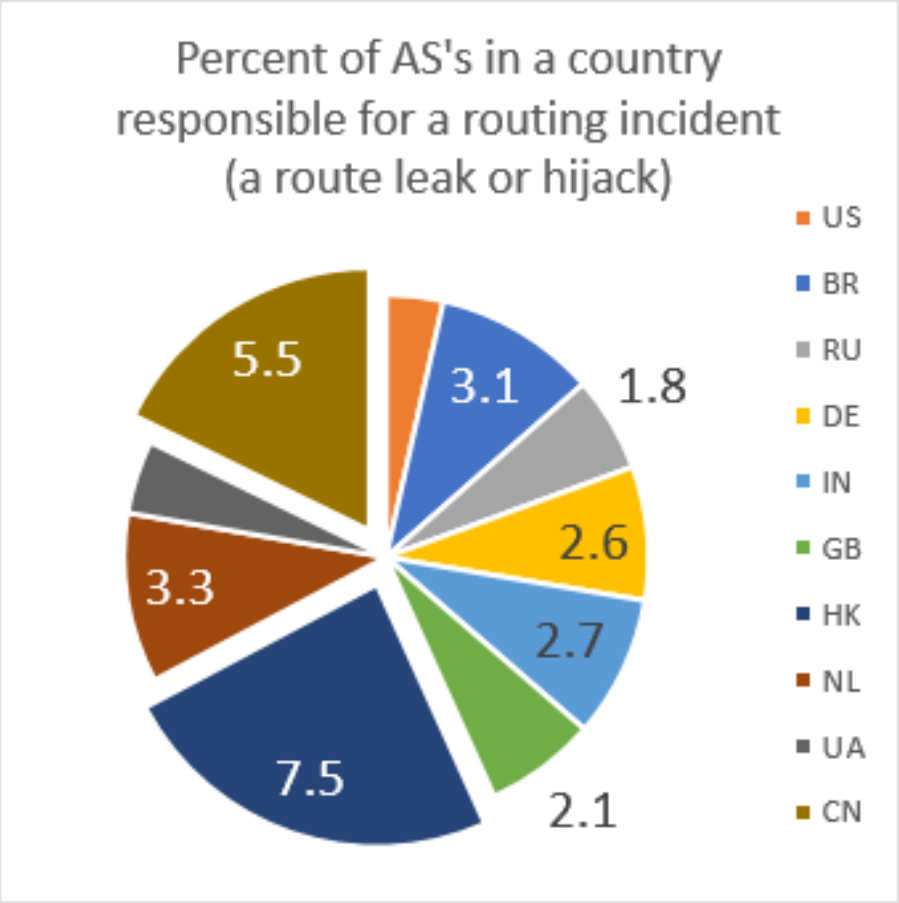
1,294 redes fueron responsables de 4739 incidentes de ruteo

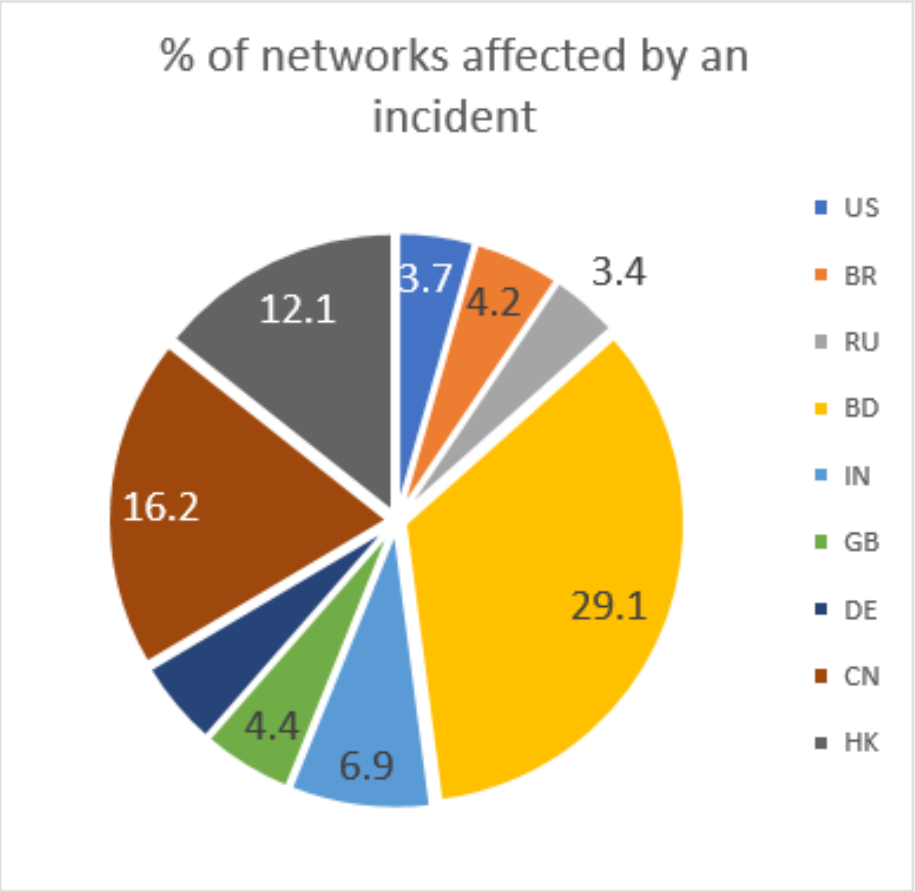
Mejora respecto de 2017, pero aun es un número alto



Fuente: https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/

Incidentes de ruteo en 2018





Fuente: https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/

Secuestro de rutas

¿Quién puede usar un recurso?

- Una organización al obtener recursos de Internet (IPv6/IPv4/ASN)
  - Indica a su upstream/peers cuales son los prefijos que va a anunciar
  - Vía e-mail, formas web, LoA, IRR (Internet Routing Registry)

Proveedores/peers: verifican derecho de uso

Whois RIRs: Información no firmada, no utilizable directamente para ruteo

Whois IRR: Información no firmada, pocos mecanismos para autentificación de derecho de uso

- La verificación <u>no siempre es todo lo meticulosa</u> que debería ser
- La integridad del sistema depende de la **<u>confianza entre peers</u>**

Secuestro de rutas

- Acción de anunciar a Internet prefijos NO autorizados.

Secuestro de rutas → Intencional.

Secuestro de rutas → Por error en la operación.

Varios secuestros de rutas vienen ocurriendo en los últimos años.

- Casos más conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - **Casos en nuestra región**

Algunos incidentes recientes

- **Abril 2017:** MasterCard, Visa y más de dos docenas de otras compañías de servicios financieros afectados
  - Grandes cantidades de tráfico fueron enrutados brevemente a través de una telco rusa.
  - Durante varios minutos, Rostelecom estaba generando 50 prefijos para muchos otros Sistemas Autónomos, secuestrando su tráfico.
- **Abril 2018:** Secuestro de DNS de Amazon mediante BGP para robar Crypto moneda:
  - eNet / XLHost (AS10297) sufrió una violación que permitió a los atacantes hacerse pasar por el servicio de DNS autorizado de Amazon.
  - Los usuarios de redes que aceptaron las rutas secuestradas (incluido el servicio DNS recursivo de Google) enviaron sus consultas DNS a un servicio DNS impostor incrustado en AS10297.
  - Si estos usuarios intentaban visitar myetherwallet.com, el servicio impostor DNS no los dirigiría a Amazon Web Services (que normalmente aloja el sitio), sino a un conjunto de direcciones IP rusas, según CloudFlare.
  - Tener en cuenta que los usuarios necesitaron ignorar las alertas de fallas de certificados en sus navegadores.
  - Ver https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/
- Estos incidentes no tuvieron éxito en los principales IXPs por estar realizando validación de origen con RPKI

RPKI

¿Qué es RPKI?

- RPKI (Resource Public Key Infrastructure)
- Validación del derecho de uso de un recurso

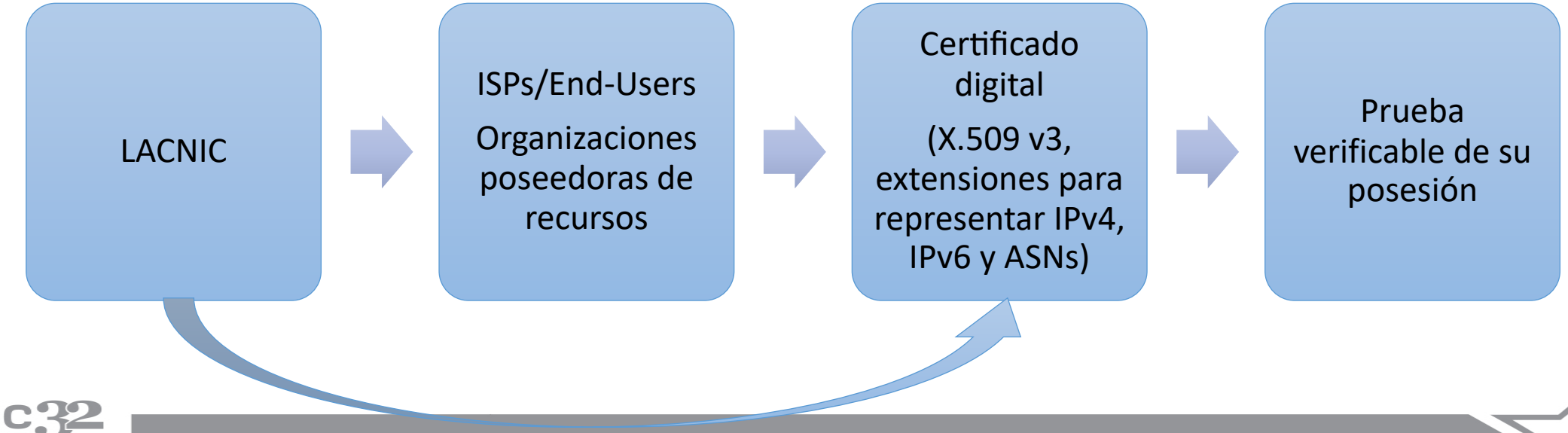
IPv4
IPv6
Sistema Autonomo

- Combina:
  - Modelo jerárquico de asignación de recursos a través de los RIRs
  - Uso de certificados digitales basados en el estándar X.509

- Estandarizado en el IETF, grupo de trabajo SIDR, RFCs 6480 – 6492
  - Gran trabajo de los RIRs en la implementación

RPKI

- Define una infraestructura de clave pública especializada para ser aplicada al enrutamiento
  - En particular, para BGP



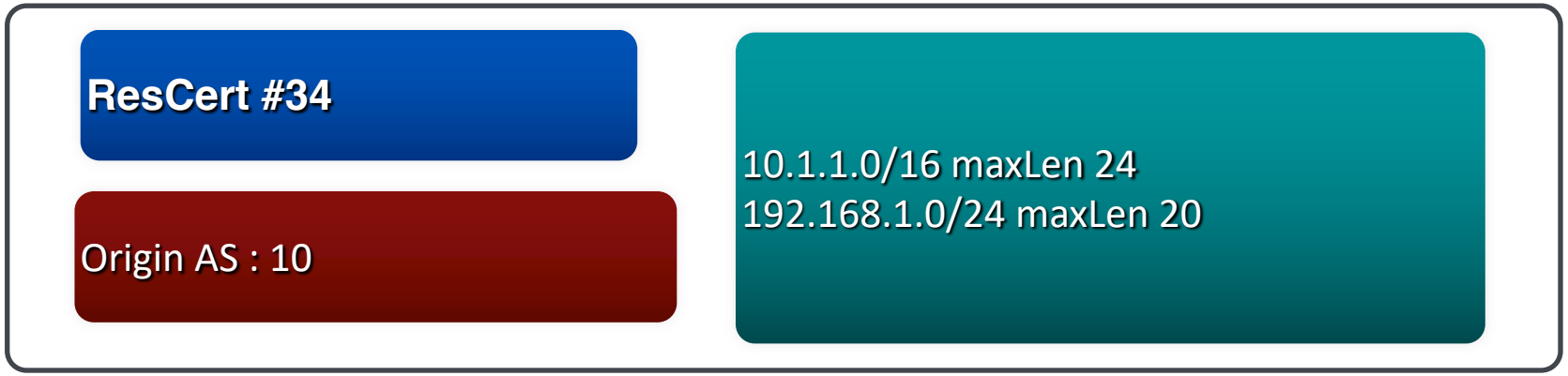
¿Qué compone la solución RPKI?

- **ROA**: Objetos firmados digitalmente para soportar seguridad del enrutamiento
  - Equivalentes a route o route6 objects de un IRR
  - Los ISPs u organizaciones pueden ***definir y certificar los anuncios de rutas que autorizan*** realizar
  - Los **ROAs** permiten definir el AS de origen para nuestros prefijos
  - **Firmados** con la clave privada del certificado
  - Toda la información es copiada en un **repositorio públicamente accesible**

- Un **mecanismo de validación** de prefijos
  - Validación de origen

ROAs

- Usando la cadena de certificados podemos firmar objetos que describan el origen de un prefijo.



- ROAs: Routing Origin Authorization
  - Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos.
  - Contienen una longitud máxima con la que puede aparecer un anuncio en Internet

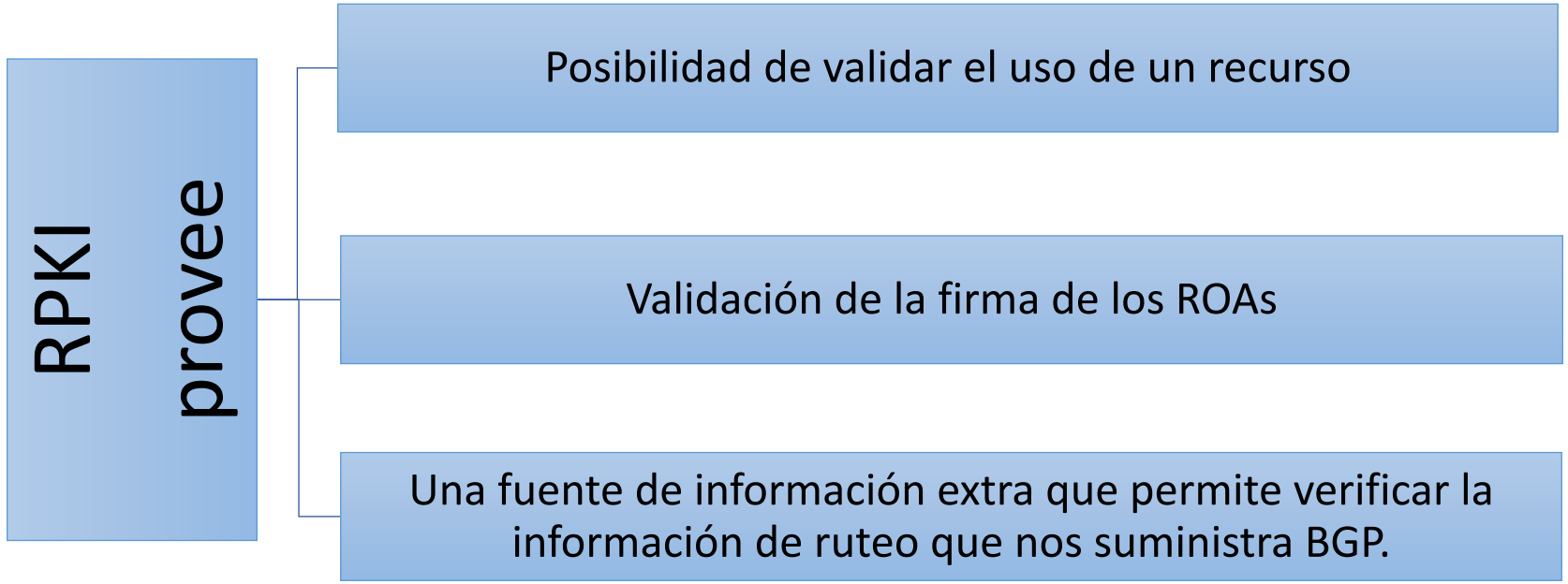
ROAs vs route(6)

- Un ROA es semánticamente equivalente a un route(6) object:
  - Asocia un prefijo a un ASN de origen
  - Con esta información es posible hacer chequeo de un anuncio BGP
- Los ROAs están firmados criptográficamente, los objetos en un IRR no
- Los ROAs no pueden ser alterados por un tercero
  - El repositorio es seguro
- RPKI sólo implementa un subconjunto de lo que un IRR puede definir

Validación de Origen

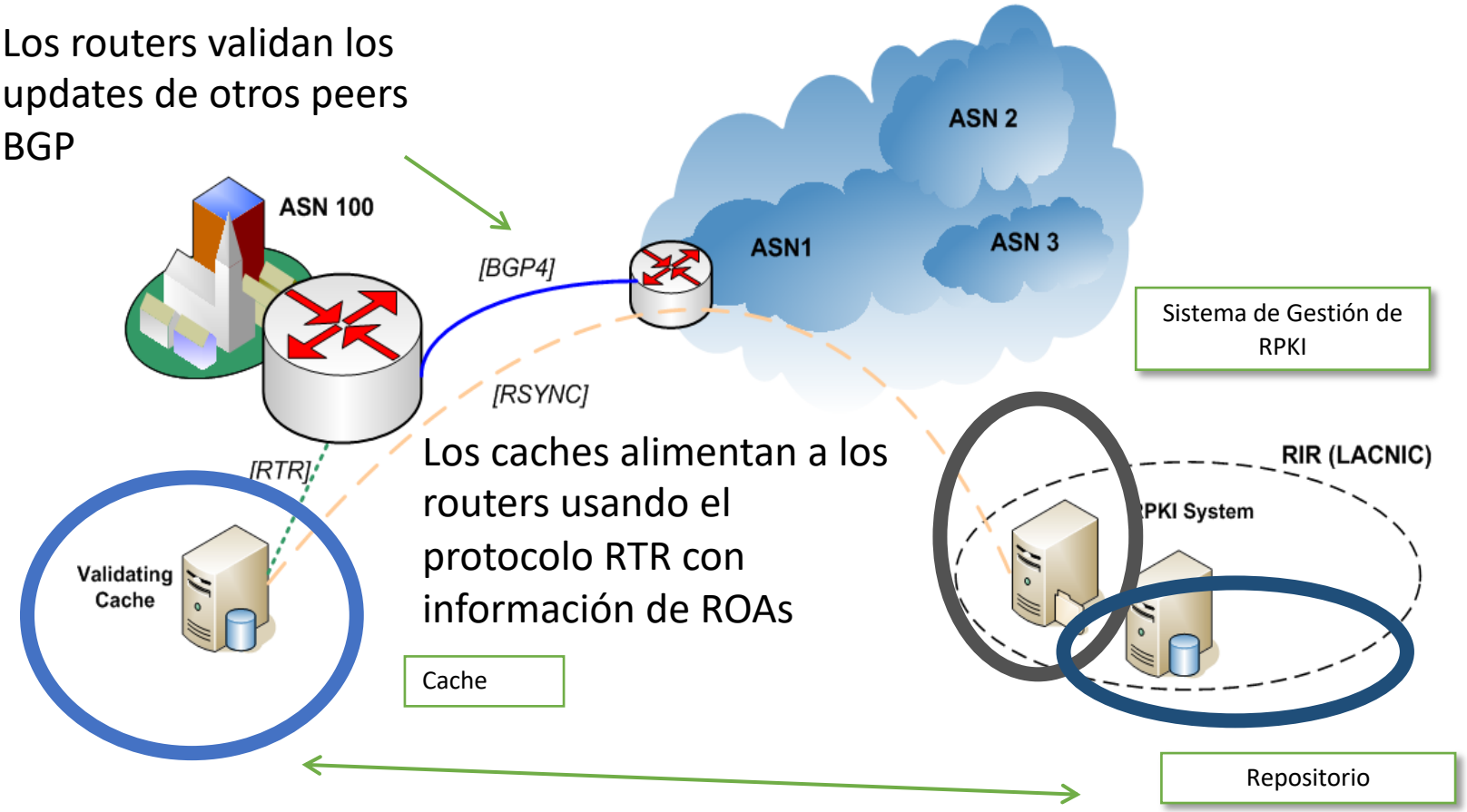
Validación

- Un router podría utilizar los ROAs para validar una ruta y eventualmente, rechazarla



RPKI en acción

Los routers validan los updates de otros peers BGP



Los caches alimentan a los routers usando el protocolo RTR con información de ROAs

Los caches traen y validan criptográficamente los certificados y ROAs de los repositorios

RPKI en acción (ii)

- El proceso de validación a nivel de la infraestructura de enrutamiento está dividido en dos
  - Validación de los ROAs como objetos firmados
    - Lo realiza el caché validador
  - Validación de la información recibida en los UPDATE de BGP
    - Lo realizan los “bgp speakers” de la red
- Existe un protocolo de comunicación entre caché y routers (RTR) que está definido en la RFC 6810, RFC8210

RPKI en funcionamiento (iii)

- En el caché
  - Se bajan por RSYNC los contenidos de los repositorios RPKI
  - Se validan los certificados y ROAs
    - Criptográficamente (cadena de firmas)
    - Inclusión correcta de recursos
- En los routers
  - Se construye una base de datos con la relación entre prefijos y AS de origen

Validación de Origen

- Una vez que los routers reciben la información de los caches, tendrán una tabla con:
  - Prefix, Min length, Max length, Origin-AS
- Aplicando un conjunto de reglas, se asigna un estado de validez a cada UPDATE de BGP
- Los operadores de red pueden usar el atributo “validez” para construir políticas de ruteo
- El estado de validez puede ser:
  - **Válido**: El AS de origen y el Largo Máximo coinciden con la información del ROA
  - **Inválido**: La información del ROA no coincide
  - **No encontrado**: No hay un ROA para el prefijo dado

Validación de Origen

UPDATE 200.0.0.0/9
ORIGIN-AS 20

VALID

max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide o el largo máximo no se respeta -> "**invalid**"

Validación de Origen

UPDATE 200.0.0.0/22
ORIGIN-AS 20

INVALID

[illegible]	[illegible]x_len]	Origin AS
172.16.0.0	/ [16-20]	10
200.0.0.0	/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide o el largo máximo no se respeta -> "**invalid**"

Validación de Origen

UPDATE 200.0.0.0/9
ORIGIN-AS 66

INVALID

[illegible]	[illegible]x_len]	Origin AS
172.16.0.0	/ [16-20]	10
200.0.0.0/[8-21]		20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide o el largo máximo no se respeta -> "**invalid**"

Validación de Origen

UPDATE 189.0.0.0/9
ORIGIN-AS 66

NOT FOUND

	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide o el largo máximo no se respeta -> "**invalid**"

RPKI en la práctica

¿Cómo definir los ROA?

- Quienes tienen recursos IPv4, IPv6, ASN:
  - Pueden hacerlo desde el sistema de administración de recursos de LACNIC (MiLACNIC)
  - Se necesita para eso los datos de usuario y contraseña de administración de recursos
- Quienes no tienen recursos propios, dependerán del ISP
- Puede haber organizaciones con recursos IP pero no ASN
  - Deben crear los ROA permitiendo a cada ASN (upstream) anunciar los prefijos
  - La creación la realiza quien posee los recursos (diferente modelo que en el IRR en el que lo hace el que posee el ASN)

¿Qué tener en cuenta?

- Verificar cómo estamos realizando los anuncios
- Ejemplo: red 203.0.112.0/22
  - La estamos publicando sumarizada?
  - La estamos publicando desagregada?
    - En bloques de qué tamaño? /23? /24?
  - Con qué sistema autónomo se originan las publicaciones?
  - Siempre es el mismos ASN?
  - Los distintos bloques se anuncian siempre con un mismo ASN?
- Importante: los ROA que creamos deben respetar esta política
- De lo contrario, estaremos invalidando nuestras publicaciones

Herramientas útiles

- Mi LACNIC: https://milacnic.lacnic.net

- ROA Wizard: https://tools.labs.lacnic.net/roa-wizard/
- ROA Announcement: https://tools.labs.lacnic.net/announcement/
- RIPE RIS: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
- BGP HE.NET https://bgp.he.net

- Documentación RPKI: https://rpki.readthedocs.io/en/latest/

¿Cómo hacer cumplir la política de ruteo?

- Usando el atributo de validez de BGP los operadores de red pueden aplicar políticas de ruteo
- Por ejemplo:
  - A las rutas con estado “valid” asignarles mayor preferencia que a las rutas con estado “not found”
  - Descartar rutas con estado “invalid”
- MUY IMPORTANTE: RPKI es una fuente de información!
  - Los operadores son libres de usarla como les parezca mejor

Interacción con BGP

- El estado **{valid, invalid, not found}** de un prefijo puede hacerse pesar en la selección de rutas

```
route-map rpki permit 10
match rpki invalid
set local-preference 50

route-map rpki permit 20
match rpki incomplete
set local-preference 100

route-map rpki permit 30
match rpki valid
set local-preference 200
```

Conclusiones

- El sistema de ruteo es uno de los pilares de Internet
  - Sin embargo, aún es vulnerable a ataques y a configuraciones erróneas
- Se ha hecho un gran avance (RPKI, Origin Validation)
- Pero es necesario seguir trabajando
  - Despliegue (Filtrado, RPKI, Origin Validation)
  - Seguimiento de la operación de RPKI: WG SIDRops de la IETF
- Los certificados de recursos y los ROAs son una herramienta para quienes tienen recursos asignados
  - Importante: firmar los recursos y definir los ROAs que especifican los anuncios de rutas

Algunas sesiones de interés esta semana

- Análisis de eventos e incidentes de ruteo recientes en Latinoamérica – Miércoles 10:30hs
- Herramientas para la visualización de información de enrutamiento - Cómo conocer y detectar incidentes de ruteo – Miércoles 11:30hs
- IRR de LACNIC: decisiones de diseño - Miércoles 12:15hs
- Validador FORT para RPKI y analisis de incidentes de ruteo – Viernes 15:00hs
- Inforedes: RIPEstat para la región de LACNIC – Viernes 15:30hs
- Tutorial de Peering: Jueves de 14:00 a 18:0

Preguntas?

Muchas gracias…