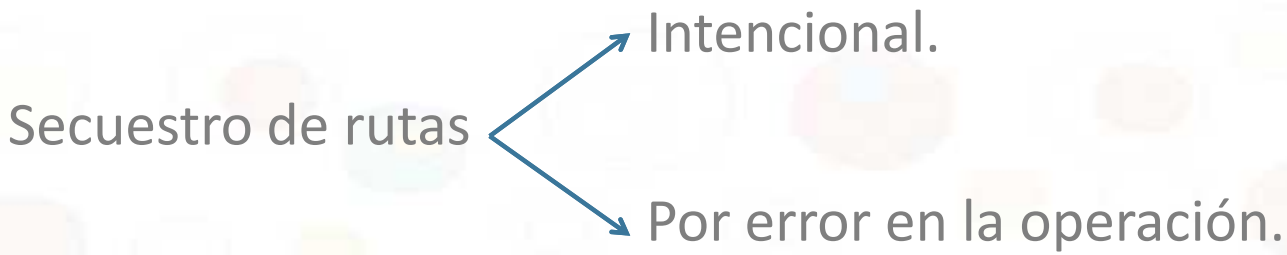
# Seguridad en el ruteo global

Guillermo Cicileo
guillermo@lacnic.net

# Secuestro de rutas

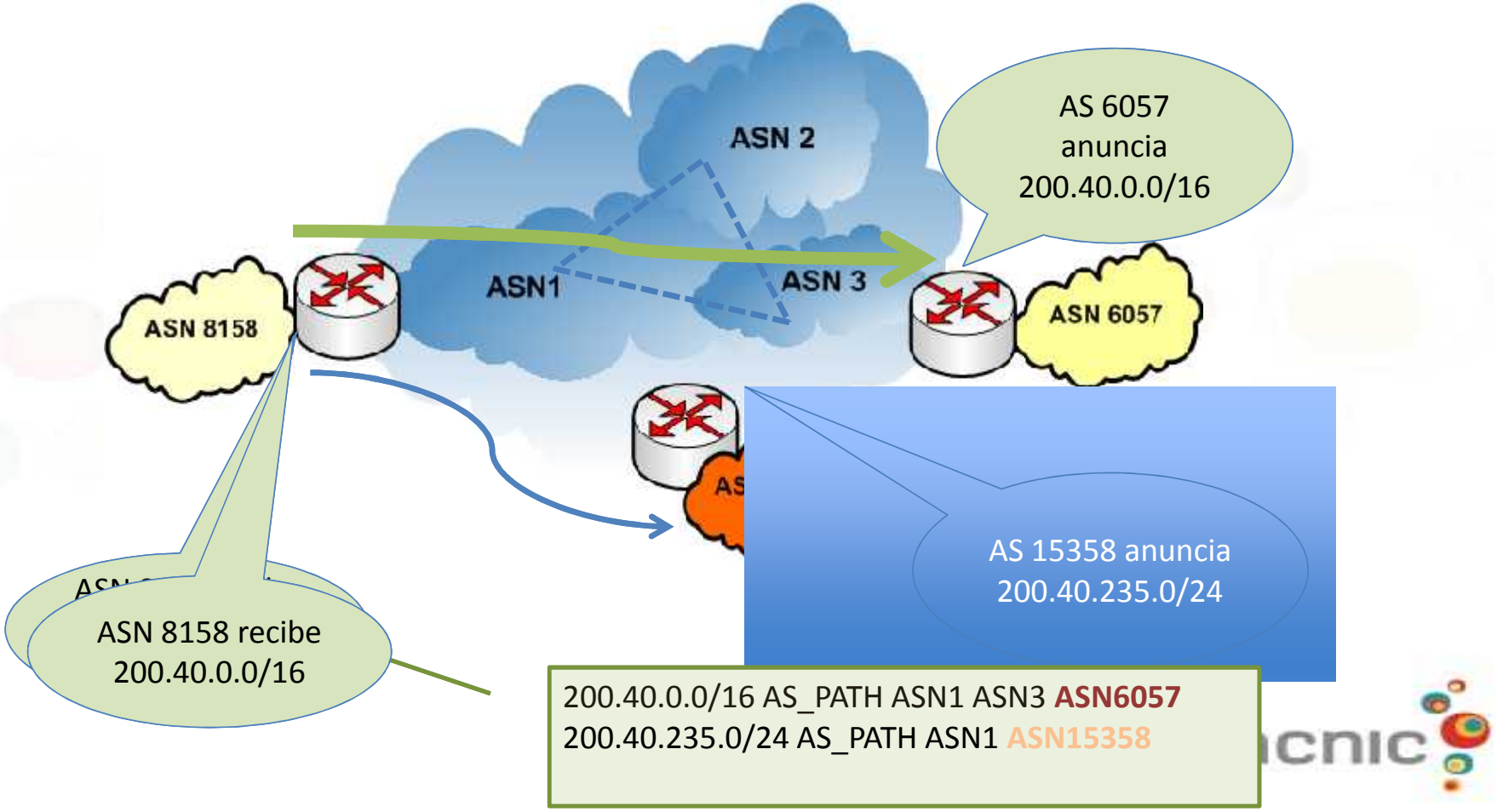
- Acción de anunciar a Internet prefijos NO autorizados.




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**

# Secuestro de rutas



# 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 hacer clic a través de las alertas de fallas de certificados en sus navegadores, pero eso no los detuvo.
  - Ver https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/

# ¿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, LoAs, 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 no siempre es todo lo meticulosa que debería ser
- La integridad del sistema depende de la **confianza entre peers**

lacnic

# POLÍTICAS DE RUTEO

# IRR – Internet Routing Registries

- Un **Internet Routing Registry** (**IRR**) es una base de datos de objetos de ruteo de Internet para determinar y compartir información sobre ruteo utilizada para configurar routers con el fin de evitar problemas en la publicación global de rutas en Internet
- Objetos diseñados para facilitar:
  - La organización de ruteo entre organizaciones
  - Proveer datos en un formato apropiado para la programación automática de routers

# IRR – Internet Routing Registries

- Existe una gran cantidad de IRRs
- El más conocido es RADB
- RADB replica todos los demas IRRs
- El atributo ”source” es el que determina cual es el registry en el que se encuentran los datos

- AFRINIC
- ALTDB
- AOLTW
- APNIC
- ARIN
- BELL
- BBOI
- CANARIE
- EASYNET
- EPOCH
- GT
- HOST
- JPIRR
- LEVEL3
- NESTEGG
- NTTCOM
- OPENFACE
- OTTIX
- PANIX
- RADB
- REACH
- RGNET
- RIPE
- RISQ
- ROGERS
- TC

# IRR – Internet Routing Registries

- Routing Policy Specification Language (RPSL) objects
  - RFC2622, RFC4012
- Principales objetos usados hoy en día:
  - AUT-NUM
  - INETNUM / INETNUM6
  - ROUTE / ROUTE6
  - AS-SET

lacnic

# RPKI

# ¿Qué es RPKI?

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

IPv4
IPv6
Sistema Autonomo

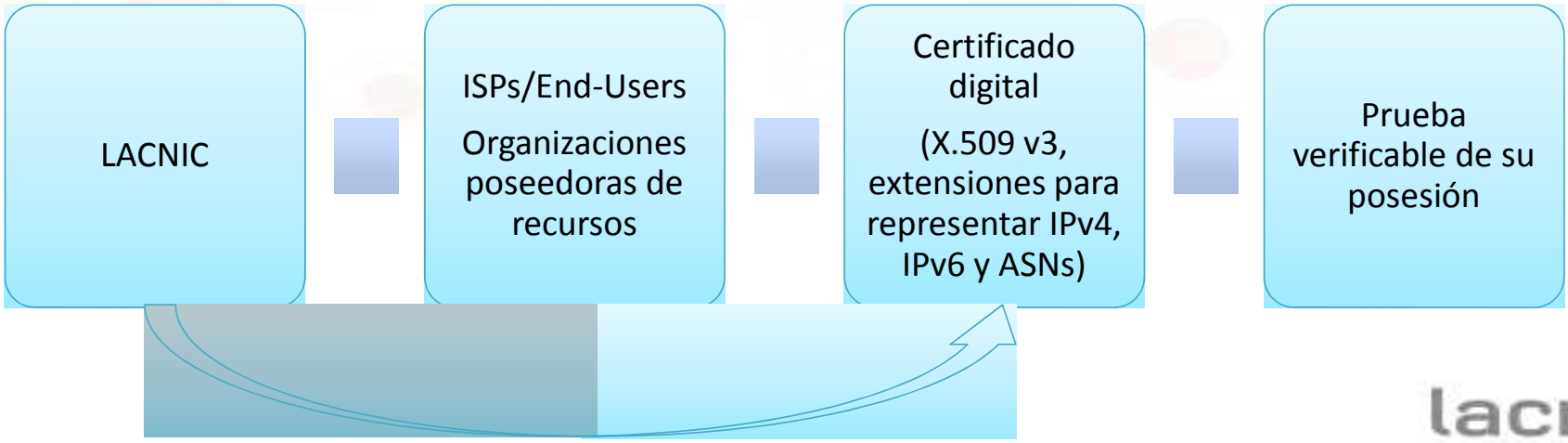
- Combina:
  - Modelo jerárquico de asignación de recursos a través de los RIRs
  - Uso de certificados digitales basados en el estándar X.509
- Estandarizado en el IETF, grupo de trabajo SIDR, RFCs 6480 – 6492
  - Gran trabajo de los RIRs en la implementación

lacnic

GC1

# RPKI

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



## Diapositiva 12

**GC1** Guillermo Cicileo, 27/07/2017

# RPKI

- Permite validar la información recibida por BGP
- Se valida que el sistema autónomo que origina los prefijos tenga autorización para hacerlo
  - Validación de origen
- Para esto se emiten certificados sobre los recursos asignados por el RIR (IPv4, IPv6, ASN)
- Se generan ROAs definiendo qué prefijos serán publicados por qué sistema autónomo
- Los ROAs definen la política de ruteo de la organización
  - Similares a los route(6) objects de los IRRs

lacnic

# TENDENCIAS ACTUALES

# Las últimas novedades

- Grandes actores comienzan a implementar validación RPKI
  - NTT, Cloudflare, próximamente mas CDNs
- La mayoría de los grandes IXPs a nivel global ya descartan rutas inválidas (RPKI)
- La información de RPKI comienza a tener preponderancia por sobre los IRRs
  - En caso de que la información difiera, la info de ROAs prevalece
- Extensión de RPKI para incorporar otras características: concepto de AS-SET, validación de relaciones customer – provider
- Generar automáticamente información en formato IRR (RPSL) a partir de RPKI

# 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 y grow 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

lacnic

# Preguntas?

Muchas gracias…