Update RPKI
Estado actual del proyecto

Resource Public Key Infrastructure

lacnog SÃO PAULO 2010 19/22 OUTUBRO 2010

Recursos de Internet

- Un ISP 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, IRR (Internet Routing Registry)
- Proveedores/peers verifican derecho de uso del recurso y configuran filtros
  - 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

Secuestro de rutas

- Cuando un participante en el routing anuncia un prefijo que no esta autorizado a anunciar se produce un "*secuestro de ruta*" (*route hijacking)*
- Malicioso u error operacional
- Casos conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - Google en Europa del este (varios AS, 2010)

Protección Actual

- Administrador de la red
  - Controles locales en su infraestructura de rutas
  - Protección de routers
  - Integridad de operación en sus protocolos de ruteo
- Medidas posibles de protección
  - Filtros 1918 (rfc1918) prefijos de redes privadas
  - "Bogon Filters" espacios no asignados de IANA
- No hay, o es muy escaso, el control de autorización de uso de un recurso en Internet

Resource PKI

- Resource Public Key Infraestructure
  - Objetivo: poder certificar la autorización a utilizar un cierto recurso de Internet
  - Mecanismo propuesto
    - Uso de certificados X.509 v3
    - Uso de extensiones para representar recursos de Internet (direcciones, ASNs)
  - Esfuerzo de estandarización:
    - SIDR working group en IETF
  - Esfuerzo de implementación
    - RIRs

Resource PKI (2)

- Metodología automatizada que permita validar la autoridad asociada a un anuncio de una ruta “origen de la ruta”
- El emisor de la información de ruta "firma" la actualización
- No permite que terceros falsifiquen la información o la firma
- Utilizar las propiedades de encriptación con Clave Pública
- Resource Public Key Infrastructure

Resource PKI (3)

- Los objetos firmados son listados en directorios públicos
- Los objetos pueden ser usados para configurar filtros en routers
- Proceso de Validación
  - Los objetos firmados son referenciados al certificado que los generó
  - Cada certificado tiene una referencia al certificado en la capa superior
  - Sigue una cadena de confianza hasta el “trust anchor”

X.509v3 con extensiones de direcciones de IP y ASNs (RFC3779)

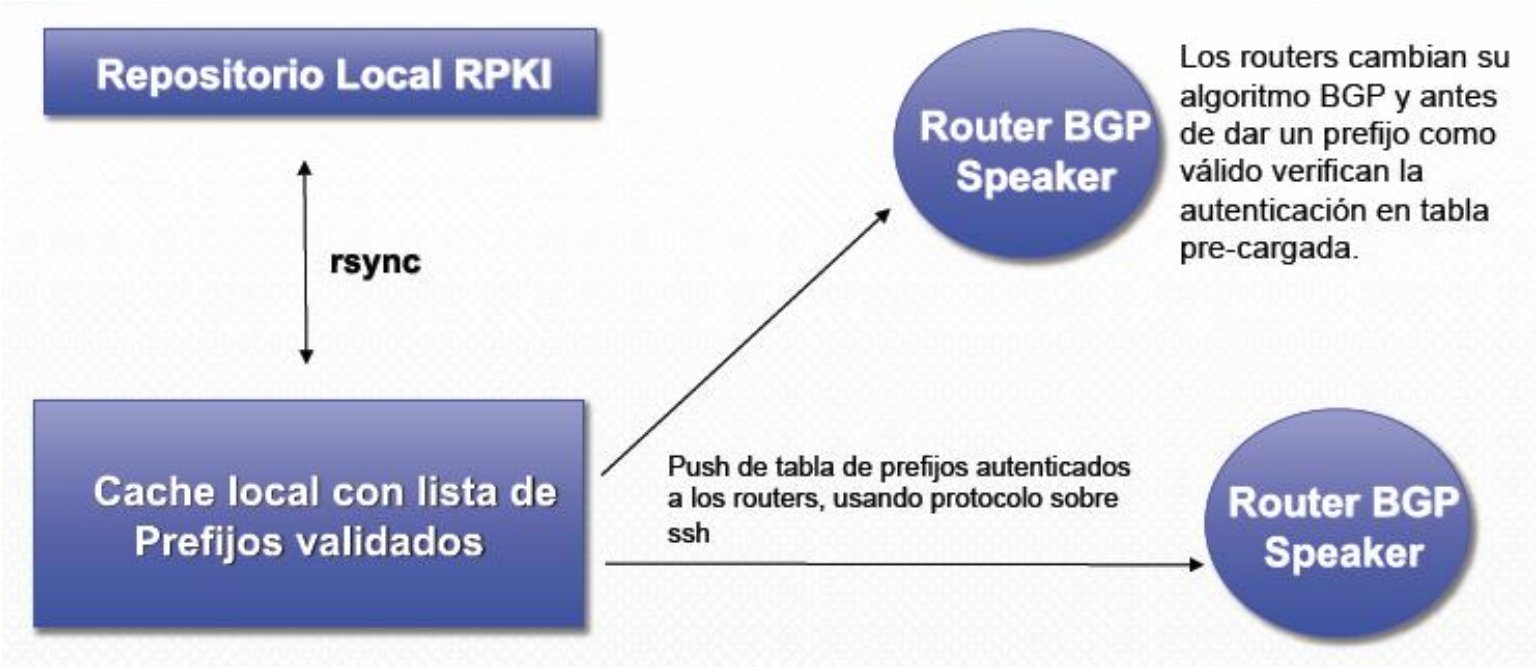
- Certificados Digitales X.509
  - n del sujeto, plazo de validez, llave publica, etc
- Con n:
  - RFC 3779 ndar IETF define n para recursos internet.
- Listado de IPv4, IPv6, ASN asignados a n

ROAs

- ROAs: Routing Origin Authorization
  - Los ROAs contienen información sobre el origen permitido de un prefijo
  - Los ROAs se firman utilizando los certificados generados por la RPKI
  - Los ROAs firmados se copian en un repositorio publicamente accesible

ROAs (ii)

- Un router podría entonces utilizar los ROAs para validar una ruta y eventualmente, rechazarla
  - RPKI Routing Protocol



Modos de operación

- Modo "*hosted*"
  - LACNIC emite los certificados y guarda en sus sistemas tanto claves publicas como privadas
    - Los certificados son emitidos a pedido de las organizaciones miembro
  - Los usuarios realizan operaciones via una interfaz web provista por LACNIC
- Modo "*delegado*"
  - Una organización tiene su propio certificado, firmado por la CA de LACNIC
  - La organización envia solicitudes de firma a LACNIC, quien se las devuelve firmadas
    - Protocolo "up-down"

Arquitectura del sistema RPKI

- CA
  - Entidad emisora de certificados (bit CA=1)
- Repositorio de certificados
  - Repositorio de certificados, CRLs y manifiestos
  - Accesible via “rsync”
- Interfaz de gestión
  - Interfaz web de usuario para aquellos que prefieran el modo “hosted”

¿Qué estamos haciendo hoy?

- El plan de ejecución de RPKI es coordinado entre los cinco RIRs
  - LACNIC, APNIC, RIPE/NCC, AfriNIC, ARIN
- Hay un conjunto de hitos acordados, algunos de los cuales ya se han cumplido
- Mayo 2010:
  - LACNIC libera el beta de RPKI
  - Se cumplió con el "*pilot release*"

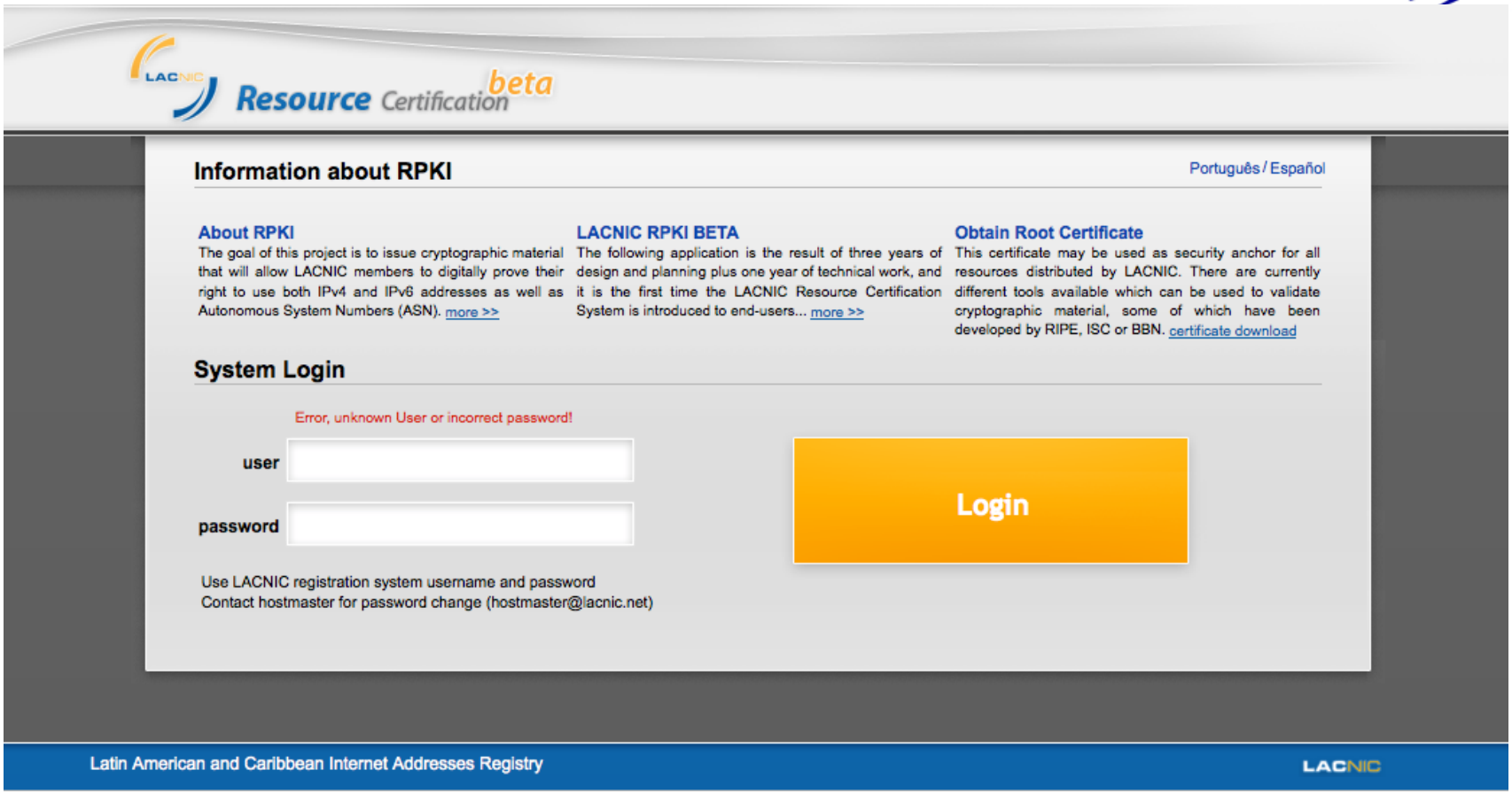
Proximos hitos

- Noviembre 2010
  - Documentos de CP y CPS (RFC 3647)
  - CP: Certificate Policy
    - Común a todas las RPKI por el momento
    - Named OID
  - CPS: Certification Practice Statement
    - Documento con consideraciones de diseño y operación relativas a una autoridad de certificación (CA)
  - Entre ambos definen caracterisiticas y procedimientos de las CAs

Próximos hitos (ii)

- Enero de 2011
  - Puesta en producción del sistema en modo "*hosted*"
    - LACNIC emitirá certificados a los miembros que los soliciten
    - LACNIC será el encargado de custodiar las claves privadas y mantener la CRL
- Durante 2011:
  - Implementación del protocolo "Top/Down"
  - Firmado sin solapamientos del espacio legado / ERX

Beta RPKI


Resource Certification beta
Information about RPKI
Português / Español
About RPKI
The goal of this project is to issue cryptographic material that will allow LACNIC members to digitally prove their right to use both IPv4 and IPv6 addresses as well as Autonomous System Numbers (ASN). more >>
LACNIC RPKI BETA
The following application is the result of three years of design and planning plus one year of technical work, and it is the first time the LACNIC Resource Certification System is introduced to end-users... more >>
Obtain Root Certificate
This certificate may be used as security anchor for all resources distributed by LACNIC. There are currently different tools available which can be used to validate cryptographic material, some of which have been developed by RIPE, ISC or BBN. certificate download
System Login
Error, unknown User or incorrect password!
user
password
Login
Use LACNIC registration system username and password
Contact hostmaster for password change (hostmaster@lacnic.net)
Latin American and Caribbean Internet Addresses Registry
LACNIC

¡Gracias!

carlos @ lacnic.net