Resource Certification

Ricardo Patara
What is it?

PKI - Public Key Certificate Infrastructure.
- Each certificated gives “authenticity” about some information.
- Contains a public key
- Signed and issued by a “trusted” entity (CA - Certificate Authority)
What is it?

Resource Certificate, aka RPKI
A PKI like others:
- Public key certificate, signed by a CA and gives authenticity about some information
- But, have some particularities
  - Extension for Internet Resources (RFC 3779).
  - Does not authenticate name/subject
What is it?

**RPKI**

- **RFC 3779**: List of IP (v4, v6) and ASN.
- Certificate to only identify “right to use” of Internet Resources

- Must not be used to identify/authenticate the identity of the certificate subject.

*Legal implications. Out of the scope*
Which is the problem?

Currently, few ways to avoid unauthorized usage of an IP block (using a IP block allocated to others)
Registration information not always updated
Information on Internet Routing Registries not always trustable
What is the problem?

- There are well known cases of “traffic hijacking” incidents.
- It has been successfully demonstrated the possibility of the “man in the middle” attack in the routing system. Without perception of main parties
- With imminent IPv4 depletion, very likely of reutilization of IPv4 addresses. “Right of use” validation to become very important.
Which is the proposal?

Main motivation: increase the security of routing system
RPKI was mechanism for a more secure infra structure
Attestation of “right to use”
“Signed objects” authorizing the announcements of IP blocks.
Which is the proposal?

X.509 Certificate

Unique ID

CA bit: on

Public key

Resources

Digital signature
Which is the proposal?

- Resource allocation/assigned followed by certificate issuance
- Each “Registry” (RIR, NIR, ISP) is a CA
- Public repository for certificates and signed objects
- Delegated and hosted system
Which is the proposal?

AFRINIC
AF. Resources
AF. Root Certificate

APNIC
AP. Resources
AP. Root Certificate

ARIN
ARIN Resources
ARIN Root Certificate

LACNIC
LA. Resources
LA. Root Certificate

RIPE
RIPE Resources
RIPE Root Certificate

IANA
IANA Resources

NIR
NIR Resources
NIR Certificate

ISP
ISP Resources
ISP Certificate

End User
E.U. Resources
E.U. Certificate

End User
E.U. Resources
E.U. Certificate

An arrow means a certificate issued for resources and signed with authoritative key of the upper entity.
Operation

Entity with the right to use of an resource
- Issues a certificate “End Entity” (bit CA off)
- Uses private key, pair of public key published on the certificate, to sign “Authorization Objects”, indicating some ASN as authorized to announce the IP blocks it has the “right to use”.
Operation

- Signed object published on the repository
- Provider uses this signed object to determine “right to use” and if they should accept or not a specific route announcement.
  - With signed object, searches for a RPKI certificate
  - Follows certification chain up to a Trust Anchor (TA).
Formalization

- IETF (Internet Engineering Task Force)
- SIDR (Secure InterDomain Routing) Working Group
Development

- RPKI is the base infrastructure
- Tools and mechanisms to implement routing system security to make usage of RPKI.
- ISPs to use those tools and mechanisms
Development

RIRs as technology promoters

- APNIC with an operation system already
- RIPE and ARIN with a beta system
Development

- LACNIC involved in the formalization process since it beginning
- More recently, dedicating big efforts to develop its system
- Dedicated staff for the project
- Java based system, in collaboration with RIPE
Development

Plans to have an operational version by end of 2009

- Web interface for keys and certificates administration
- Objects signing
- Repository
- Following plans: “TOP/DOWN”
As mentioned, this is only the basic infrastructure. Tools will be needed in order to create routing security mechanisms. Community participation/collaboration needed (ISPs in general).
Participation

To try the system
To participate and collaborate on the formalization process
To propose tools and solutions
Comments, questions?