RPKI Operations

nanog65 - morrowc@google.com

Agenda

- Basic overview of deployment
- Systems Management
- Extensions for route filtering today

(skilled operators note no legal discussion, no ‘signing paperwork’ discussion)

What is RPKI?

- Number Resource Public Key Infrastructure
- A PKI to help validate who should be using which IP number resources
- Rooted at the RIR's (or maybe IANA later?)
- RIR's allocate numbers to their customers, who assign numbers to their customers… turtle train!
- RPKI data should follow that hierarchy, data is published via rsync
  - today rsync, tomorrow http!
- Cert mish/mash aside you are running a public rsync server

Other longer presentation(s):

RIPE60 - http://goo.gl/fay4SB && Apricot 2014 - https://goo.gl/50lwPa

Systems Management

You said rsync server?

- rsync server
- key management (certs/keys/etc)
- data to be published to the world

Probably not all on one ‘server’, maybe not all openly accessible?

Systems Management

A simple proposal to get you started:

- One server (sure, make a backup), protected from the outside, with keys and master data sets
  - use reference software platform (http://rpki.net/wiki/doc/RPKI/Installation one-page-install)
  - there is only one publicly available CA suite
- More (2? 3?) publicly available servers for other participants to gather published data
  - puppet framework (https://github.com/google/rpki-mgmt)
  - manages rsync configuration, management user accounts, general puppet stuff
- More (3?) gathering systems to collect external party RPKI data
  - follow the publication hierarchy, collect and digest for use in other tasks

Extensions for route filtering today

- Do you manage route filters for your customers?
  - From IRR data?
  - From email?
  - worse?

Extensions for route filtering today

- Is IRR/your data always accurate?
- Do customers ever remove prefixes from the IRR?
  - NIST report on data quality: http://goo.gl/cTpO3w
  - RIPE report on data quality: https://goo.gl/rqOFdS
- Use the RPKI data collected to determine correct changes to IRR data prior to filter installation
  - example service: whois.rpki.net
    - check your IRR results against published ROA content
    - auto-clean your customer's data for them (in your view)
- Use an off-path device to check policy based on ROA content against the routing table data, mark/preference/count/collect
  - no danger to your network, data collection to inform your future plans

Questions?