Changes to RP / CA Expectations

Chris Morrow
sidrops whipping persona

TEXT FOR DISCUSSION

Please review:

https://mailarchive.ietf.org/arch/browse/sidrops/?gbt=1&index=04s5QYa_BdVNrfC6TH4Axr7izqs

RP/CA Expectations today

CA publishes ‘things’.

RP software downloads these.

If there are mismatched expectations:

- Some RP software ‘patches’ things up
- Different assumptions/actions per package

This results in chaos!

Let's Set GroundRules

- A CA should publish at least this minimal set of items atomicly:
  - 1 x Manifest
  - 1 x CRL
- A CA MAY publish additional items
  - EE-certs for router/asn/etc
  - ROA
- If an RP's view of a CA does not include the minimal set, the CA in question is entirely excluded from OV calculations
  - There is no 'fix up' possible

Why the minimal set?

- Simple to reason about
  - MFT - complete list of repository items
  - CRL - complete list of revoked items from past data
- Clear demarcation between what the CA’s routing intent is
- Clearly demarcate the responsibility of the RP

What about Cached Items?

- Used if not
  - On the CRL
  - Still valid (time)
  - Still valid (certificate details are correct)
- Object IS on the Manifest
- Why trust the cached items?
  - Prevents an attacker from removing RRDP/RSYNC items in flight

Current status of software

- OpenBSD rpki-client, FORT are ‘fixed’
- routinator (v0.8.0) - working toward -bis functionality
- Rpstir - working toward -bis functionality
- RIPE NCC Validator, OctoRPKI have issues lodged, no action todate (06/24/2020)

Feedback for:

Downloaded items should be all of items in MFT
Using in cache and alerting when cache is used