IETF 86
RPKI Validator Testing

2013 March 12, Orlando, FL

Andrew Chi <achi@bbn.com>

Participants: Rob Austein (DRL), Oleg Muravskiy (RIPE NCC), David Mandelberg (BBN), Andrew Chi (BBN)

Participants

- **The Usual Suspects (RPKI validators. Please join us!)**
  - RPSTIR (BBN): http://sourceforge.net/projects/rpstir/
  - Rcynic (R. Austein): http://rpki.net/
  - RIPE NCC validator: http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources

- **Data set: 13 trust anchors, 7983 files**
  - CA certificates: 2239 (includes TA certs)
  - CRLs: 2233
  - ROAs: 1271
  - Manifests: 2234
  - Ghostbusters: 6

Trust Anchors

Production

- rsync://rpki.afrinic.net/repository/AfriNIC.cer
- rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin.cer
- rsync://rpki.apnic.net/repository/apnic-rpki-root-arin-origin.cer
- rsync://rpki.apnic.net/repository/apnic-rpki-root-afrinic-origin.cer
- rsync://rpki.apnic.net/repository/apnic-rpki-root-lacnic-origin.cer
- rsync://rpki.apnic.net/repository/apnic-rpki-root-ripe-origin.cer
- rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
- rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
- ARIN trust anchor (https://www.arin.net/public/rpki/tal/index.xhtml)

Test/Older

- rsync://rpki.apnic.net/repository/APNIC.cer
- rsync://apnicrpki.rand.apnic.net/repository/root.cer
- rsync://repo0.rpki.net/rpki/root.cer
- rsync://localcert.ripe.net:10873/ta/localcert-ripe-ncc-nonhosted-pilot.cer

Nota Bene

- **Time synchronization for testing.** Since time cannot be stopped, validators must be run (nearly) simultaneously, or system clocks must be set to (nearly) the same time. Reproducing exact results hours later is tricky.

- **Need ghostbusters (and software support).** We currently know everyone to contact, but this won't be the case forever. Also, this gets old: "Look at lkFMoy8y-gcZpVsclY2963tfViY.cer." "Say that again?" Better might be: "Look at the cert issued by RIPE-NCC to RIPE-member-314." The validator testing session was rowdy enough that we were told to get a room. There are now "quiet" signs in the terminal room.

- **Differences in validators** mean that the default configurations yield slightly different results.

Some Validator Differences

	rcynic (Austein)	RPSTIR (BBN)	RIPE NCC
Manifest/CRL strictness	Strict CRL. Reject publication point objects if bad CRL. Warn if bad MFT.	User configurable. Warn by default for bad/stale MFT or bad/stale CRL.	Strict. Reject all publication point objects if either MFT or CRL is bad/stale.
Scope: what files are evaluated?	Files within valid SIA directories.	All downloaded files.	Files listed on valid MFTs.
Ghostbusters support	Yes	No (as of Mar 2013)	No (as of Mar 2013)

RFC 6481 (Repository Structure) and RFC 6486 (Manifests) provide a good base framework and specify which options are left to local policy. Additional guidance for both CAs and RPs could make the **default behavior** more uniform.

Bugs Identified and/or Fixed

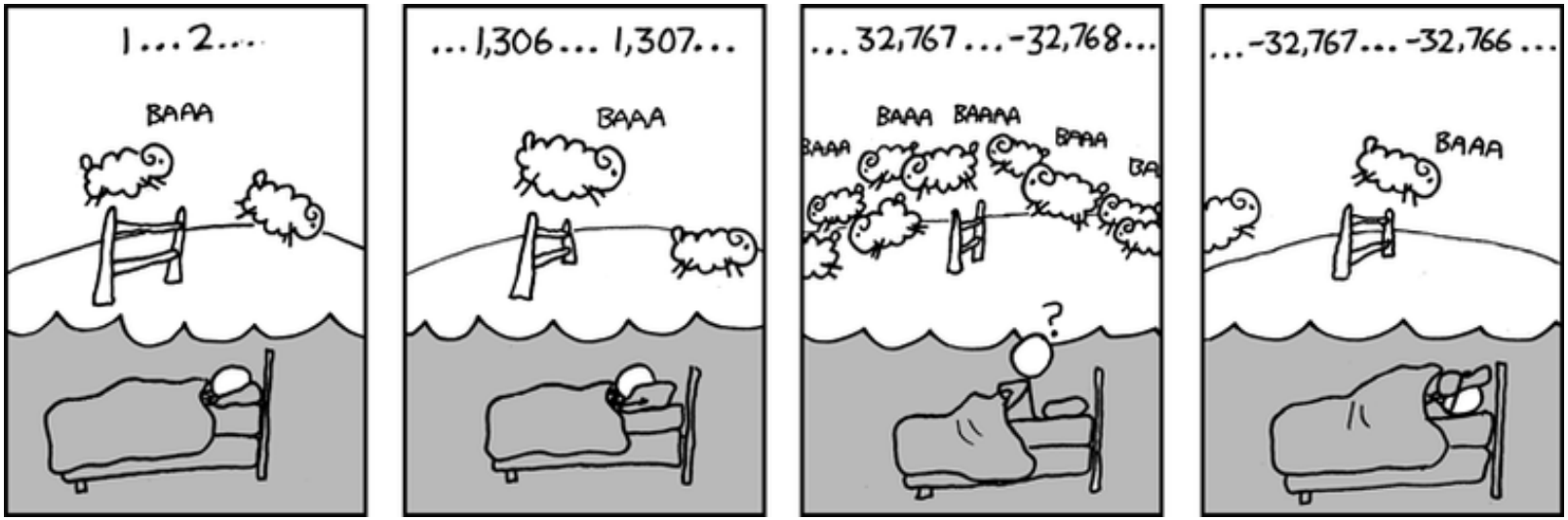
Validators

- RPSTIR: should reject manifests whose EE certs have an empty (not inherit) RFC 3779 extension.
- Rcynic: should check CRL Issuer against parent cert Subject
- RIPE NCC: should not reject manifests listing ghostbusters

Repositories

- Some “orphaned” objects are still accessible via rsync.
- Some expired or revoked objects are still present.
- Some missing SIAs in MFTs (but MFT SIA is self-referential).
- Some reference mismatches: CRL issuer ≠ parent cert subject. (Already fixed! Thank you, LACNIC.)

Questions and comments



Sheep overflow