

Update on RPKI Validator Testing

SIDR WG – IETF 85, Atlanta, GA
Andrew Chi <achi@bbn.com>
BBN Technologies

Outline

- ⦿ RPKI Validator Testing at IETF 85
- ⦿ BBN Recent Runtime Statistics
- ⦿ BBN Validator Test Harness

IETF 85 Validator Test Setup

- ⊗ Validators
 - ⊗ **rcynic** - <http://subvert-rpki.hactrn.net/trunk/rcynic/>
 - ⊗ **BBN RPSTIR** - <http://sourceforge.net/projects/rpstir/>
 - ⊗ **RIPE NCC Validator** - <http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources>
- ⊗ Trust anchors (TAs)
 - ⊗ Production TAs from **all five Regional Internet Registries**
 - ⊗ Pilot/Experimental TAs
- ⊗ Repository snapshot taken on Monday, 5 Nov 2012
 - ⊗ ~10,000 objects: 3k certs, 3k manifests, 3k CRLs, 1k ROAs
 - ⊗ Test was run on the same offline snapshot to avoid time skew.

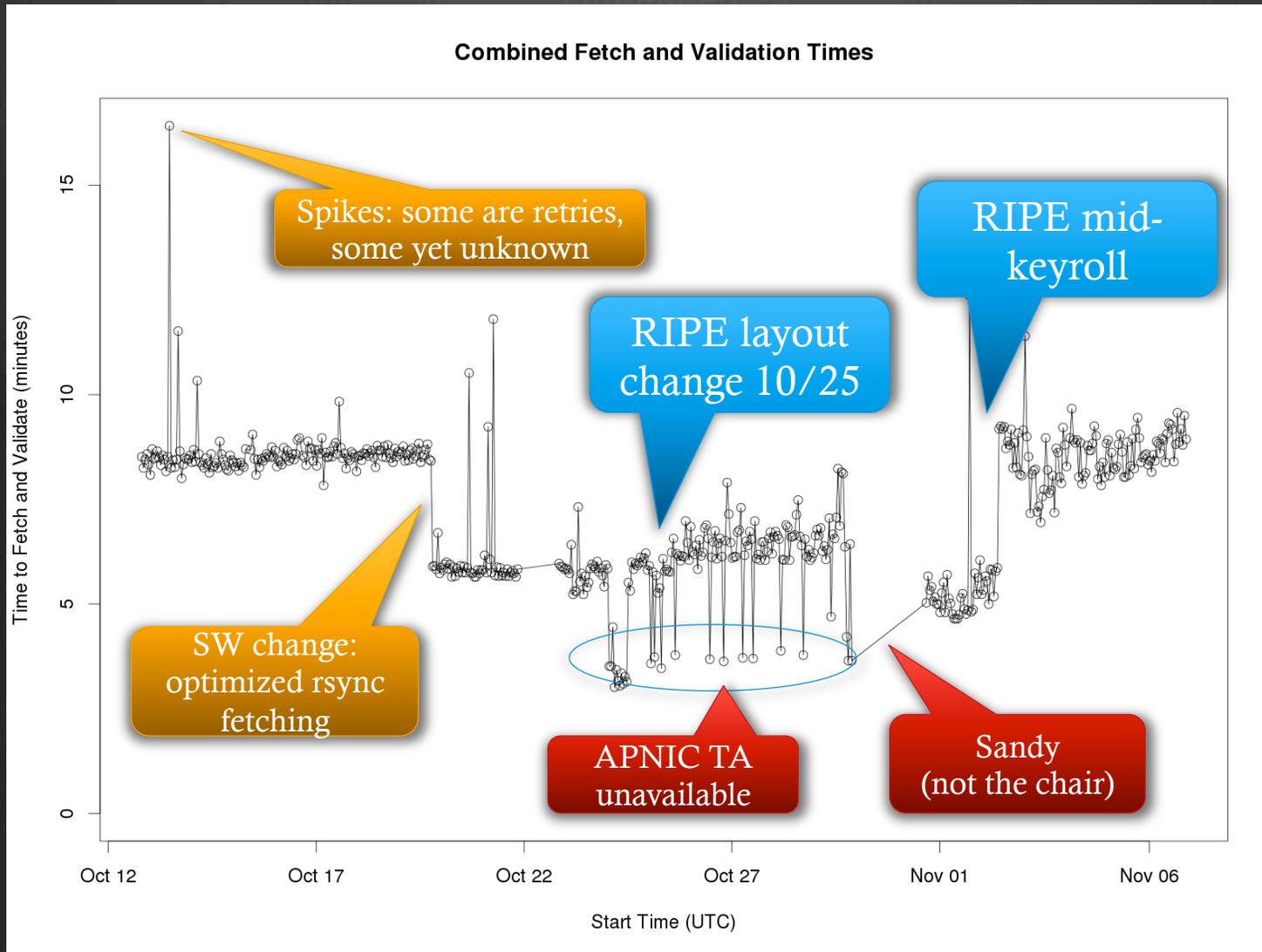
Validator Test Results

- ⊗ Nearly all 10,000+ objects were validated by all 3 implementations. Production repositories are fine, modulo known minor nits.
- ⊗ RPSTIR and rcynic results were nearly identical, RIPE NCC differed only slightly more. Small handful of discrepancies between results, mostly in pilot repos (~10)
 - ⊗ Differing strictness about manifest/CRL staleness
 - ⊗ Differing strictness about MFT EE SIA pointer, filename ext.
 - ⊗ Ghostbusters support
 - ⊗ A couple of bugs (1 RIPE, 1 BBN)
- ⊗ **SUCCESS:** The production Resource PKI is nearly 100% compliant with the SIDR RFCs. We have multiple interoperating implementations: 5 producers x 3 consumers.

BBN Validation Run Time Stats

- ⊗ BBN RPSTIR periodically sweeps all 5 RIRs. As of IETF 85, this is about 10,000 objects.
- ⊗ Caching is disabled – therefore, worst case scenario with no memory of previous fetches.
- ⊗ Retry on rsync error, with multiplicative backoff. No retry on validation errors.
- ⊗ 24 parallel rsync threads
- ⊗ Note: RPSTIR is designed to pipeline rsync fetching with certificate validation in order to reduce overall run time.
Current release: rpstir-0.5

BBN Validation Run Time Stats



BBN Validator Test Harness

- ⊗ Previously, BBN produced over 200 single-object conformance torture cases for strictly compliant validators (and therefore, repositories).
 - ⊗ TA: `rsync://rpki.bbn.com/conformance/root.cer`
- ⊗ To further harden validators for production use, the next step is to create a test harness for time-varying, multi-object scenarios.
- ⊗ The test harness (work-in-progress) simulates the evolution of a repository through a series of “epochs” in time, allowing the simulation of scenarios such as:
 - ⊗ Fetching during various stages of key rollover
 - ⊗ Fetching during a publication point update

RPKI Epoch Builder (alpha)

Epochs

- Epoch 0
 - Validity Start Time of Allocation ini-iana
 - Publication Time of Allocation ini-iana
- Epoch 1
 - Validity Start Time of Allocation ini-APNIC-1
 - Publication Time of Allocation ini-APNIC-1
 - Publication Time of Allocation ini-RIPE-2
 - Validity Start Time of Allocation ini-RIPE-2
 - Validity Start Time of Allocation ini-AFRINIC-0
 - Publication Time of Allocation ini-AFRINIC-0
- Epoch 2
 - Validity Start Time of Allocation ini-LIR-4
 - Publication Time of Allocation ini-LIR-4
 - Publication Time of Allocation ini-LIR-8
 - Validity Start Time of Allocation ini-LIR-8
 - Publication Time of Allocation ini-LIR-2-2
 - Validity Start Time of Allocation ini-LIR-2-2
 - Validity Start Time of Allocation roa-ini-RIPE-2
 - Publication Time of Allocation roa-ini-RIPE-2
 - Validity Start Time of Allocation ini-LIR-1-2
 - Publication Time of Allocation ini-LIR-1-2
 - Publication Time of Allocation ini-LIR-3
 - Validity Start Time of Allocation ini-LIR-3
 - Publication Time of Allocation roa-ini-AFRINIC-0
 - Validity Start Time of Allocation roa-ini-AFRINIC-0
 - Publication Time of Allocation ini-LIR-3-1
 - Validity Start Time of Allocation ini-LIR-3-1
 - Publication Time of Allocation ini-LIR-0-1
 - Validity Start Time of Allocation ini-LIR-0-1
 - Publication Time of Allocation ini-LIR-6
 - Validity Start Time of Allocation ini-LIR-6
 - Publication Time of Allocation ini-LIR-0-2
 - Validity Start Time of Allocation ini-LIR-0-2
 - Publication Time of Allocation ini-LIR-7
 - Validity Start Time of Allocation ini-LIR-7
 - Validity Start Time of Allocation ini-LIR-9

Allocate ini-APNIC-1: [as:r%536870912, ipv4:r%13, i...

Allocation Id: ini-APNIC-1

Issuer: IANA-0 [Edit]

Subject: IANA-0.APNIC-1 [Edit]

Deallocation Publication Time | Validity End Time

Allocation Publication Time | Validity Start Time

Predecessor Epoch Events

Validity Start Time of Allocation ini-iana

[Remove] [Add...]

Coincident Epoch Events

Publication Time of Allocation ini-APNIC-1

[Remove] [Add...]

Successor Epoch Events

Validity End Time of Allocation a1
Validity Start Time of Allocation a1
Validity Start Time of Allocation ini-LIR-0-1
Validity Start Time of Allocation ini-LIR-1-1
Validity End Time of Allocation ini-APNIC-1
Validity Start Time of Allocation ini-LIR-2-1
Validity End Time of Allocation a2
Publication Time of Allocation a1
Publication Time of Deallocation a1
Publication Time of Deallocation a2
Validity Start Time of Allocation a2
Validity Start Time of Allocation roa-ini-APNIC-1
Publication Time of Allocation a2
Cache Check 1

[Remove] [Add...]

Allocations

INR Type:	as	Range:	r%536870912	Delete
INR Type:	ipv4	Range:	r%13	Delete
INR Type:	ipv4	Range:	p%268435456	Delete

[Add Action] [Delete Action] [Expand] [Apply] [Reset] [Exit] [Run] [Save]

Example Test Harness Scenarios

- ⊗ Nominal Scenarios
 - ⊗ Hierarchical vs shallow repositories
 - ⊗ Certificate expiration, revocation, refresh
 - ⊗ Key rollover
- ⊗ Error Scenarios
 - ⊗ Invalid signatures and RFC 3779 violations
 - ⊗ Publication point not accessible
 - ⊗ Publication point in mid-upload state
 - ⊗ Evil-twin multiple parent, and others
- ⊗ Error Recovery Scenarios
 - ⊗ Publication point in mid-upload state for first fetch
 - ⊗ Expired parent is replaced by non-expired parent

Questions?

