Measuring RPKI Repositories

JaNOG / Kurashiki
2012.05.06

Randy Bush <randy@psg.com>
Don’t Panic

• I am an Engineer, we always think about the problems
• I am a Researcher, we are only interested in the problems
• The RPKI is going really well
• But I want to talk about the problems
Review of RPKI Structure
Publishing / Issuing Party

GUI

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

<table>
<thead>
<tr>
<th>AS</th>
<th>Prefix</th>
<th>Max Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>3130</td>
<td>98.128.1.0/24</td>
<td>24</td>
</tr>
</tbody>
</table>

Create | Cancel

Matched Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Origin AS</th>
<th>Validation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>98.128.1.0/24</td>
<td>4108</td>
<td>Route</td>
</tr>
<tr>
<td>98.128.1.0/24</td>
<td>3100</td>
<td>DNS</td>
</tr>
</tbody>
</table>

Up / Down to Parent

Up / Down to Child

Publication Protocol

Resource PKI

IP Resource Certs
ASN Resource Certs
Route Origin Attestations

RPKI Certificate Engine
Issuing Parties

IANA

APNIC

IIJ

Resource PKI

SIA Pointers

GUI
Issuing Parties

IANA

APNIC

IIJ

Relying Parties

RCynic Gatherer

Validated Cache

NOC Tools

BGP Decision Process

Pseudo IRR

route: 147.28.0.0/16
descr: 147.28.0.0/16-16
origin: AS3130
notify: irr-hack@rpki.net
mnt-by: MAINT-RPKI
changed: irr-hack@rpki.net 20110606
source: RPKI

route:   147.28.0.0/16
descr:   147.28.0.0/16-16
origin:  AS3130
notify:  irr-hack@rpki.net
mnt-by:  MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:  RPKI

2012.07.06 JaNOG RPKI Measure
My Routing Relies on It!

• If my routing relies on the RPKI, then I care a lot about publication reliability

• Of course, good relying party software will expect failures, so this is not a killer

• But when we look at current publication, much is not operational quality

• This has to be fixed
These Graphs are from rpki.net's Relying Party Software Web Page it Makes for You.
Not Bad

An ISP

pubd-pilot.lab.dotag.de last week

- Sync time (success): 3.14s
- Average sync time (seconds): 3.14s
- Average connection count: 1.00
- Average object count: 3.00

An RIR

repository.lacnic.net last week

- Sync time (success): 945.96s
- Average sync time (seconds): 945.96s
- Average connection count: 63.62
- Average object count: 254.00

2012.07.06 JaNOG RPKI Measure
Not So Good
• They do not monitor and have no real NOC
• They do not work weekends
• I had to write a friend in APNIC Engineering
RIPE Stayed Up

Repository details for rpki.ripe.net 2012-07-03T23:10:13Z

<table>
<thead>
<tr>
<th>Details</th>
<th>Current .cer</th>
<th>Current .crl</th>
<th>Current .mft</th>
<th>Backup .roa</th>
<th>Current .roa</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate has expired</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1033</td>
</tr>
<tr>
<td>Bad key/Usage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>Certificate failed validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>CRL not yet valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>CRLDP doesn't match issuer's SIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>Manifest not valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>Object rejected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>EEs certificate with 1024 bit key</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>Nonconformant X.509 issuer name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1033</td>
</tr>
<tr>
<td>Nonconformant X.509 subject name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>101</td>
</tr>
<tr>
<td>RSync partial transfer</td>
<td>17</td>
<td>6</td>
<td>500</td>
<td>517</td>
<td></td>
<td>1036</td>
</tr>
<tr>
<td>Stale CRL or manifest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>Tainted by stale CRL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>Tainted by stale manifest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>Tainted by not being in manifest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>Non-sync URI in extension</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3833</td>
</tr>
<tr>
<td>Object accepted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>RSync transfer succeeded</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1035</td>
</tr>
<tr>
<td>rsync transfer succeeded</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1035</td>
</tr>
</tbody>
</table>

rpki.ripe.net over last week

Average sync time (seconds): 2269.75
Sync time (total failure):
RIPE has Bad History

• This was an NFS problem (NFS is Evil!)
• It went on for months
• RPKI.NET logs had full detail showing “NFS”
• But “Nothing Can Be Wrong at the RIR”
• Finally it was fixed, but small problems remain
The RIRs are Not Network Operators

They're PTTs, “There can be no problem”
Good Software Will Save US

- Of course, good relying party software will expect failures, so this is not a killer
- rpki.net relying party software uses old data if it can not fetch new
- As RPKI data are fairly stable, this is OK
- But RIPE’s in-addr disaster lasted five days!
Some Statistics

Again, from rpki.net
Relying Party Software
Connect Time (linear)

RIPE & APNIC Very Slow
Deliberately Bad Directory Structure
Connect Time (log)

It Can Be Done Well
Connection Counts
Number of Objects

This is Good!!!
Conclusions

• RPKI Deployment is serious, especially in the RIPE region
• RIRs are not Operator Quality/Reliability
• JPNIC could set an example!
• APNIC & RIPE Publication Structure needs to be fixed
• Relying Party software works around these
• More Measurement and Monitoring