RPKISpider

Eric Osterweil
Danny McPherson
Getting from A to B: Who is allowed to do what?

• BGP runs by rumor
  – Participants assert reachability and "gossip" about what they’ve heard from each other

• We’ve lacked a rigorous way to automatically learn:
  – Who is the rightful holder of a resource?
  – Who is allowed to assert reachability for resources?
  – What’s a "resource!?!?"

• We’ve always needed number resource certification
  – A stepping stone towards answering: "who is allowed to do what?"
Resource Certification

• Being able to verify the authorized resource holders
  – IP addresses are allocated hierarchically
  – Announcements and routing are authorized by resource holders (bilaterally)

• The Resource Public Key Infrastructure (RPKI) is one incarnation of number resource certification
  – It largely focuses on “routed resources” (i.e., ROAs)

• The envisioned usage for RPKI has morphed from just Internet number resource titleship to routed resource certification
  – That is, BGPSEC uses RPKI to sign and verify BGP updates and a new BGP path attribute
• IP addresses are allocated hierarchically
  – So, represent that w/ crypto objects

• RPKI envisions an IANA trust anchor that delegates resource allocations to RIRs
  – RIRs then sign objects for their allocations
  – But... We don’t have a global root today, so we have added complexity

• So... A prefix may have been allocated from IANA to ARIN to Level(3) to a customer...

http://rpkispider.verisignlabs.com/
Deployments have started...

- Can we operationalize RPKI (repositories and RPs)?

- We should be measuring!

- Designs should accommodate fully deployed system (i.e., at least operate at scale of today’s Internet routing system)

- Discussions about scaling have already begun
  - “Sizing Estimates for a Fully Deployed RPKI” Verisign Labs tech report #1120005 v2
    http://techreports.verisignlabs.com/tr-lookup.cgi?trid=1120005&rev=2
  - Some other work has verified these results
Outline

• How does RPKI work?

• How has RPKI been working?
How does RPKI work?

• Caches try to get info from authorities, and keep it near RPs
  – Chains start from Trust Anchors
  – Trust Anchors are certificates
  – Certs point to manifests

• Basically, one big crypto certified DB: lot’s of referential integrity needed

• Chains of objects point at each other, and they use opaque hash values as names
  – If something gets borked, or a directory is misnamed, it is not human readable, so not easy to detect…
RPKISpider

• Backend is parallelized RP cache gathering (spidering) system
  – Ground up implementation

• RPKISpider has been running for a few months
  – http://rpkispider.verisignlabs.com/
  – Follow us on Twitter! @RPKIUpdateBot

• What we track
  – Transaction success rates, throughput, etc.
  – Delegation structure
  – Object count, distribution of object types, etc.
  – Portion of covered routed space
What we’ve seen...

• Growth: up and to the right
  – Overhead: roughly 10k objects for just 1,200 ROAs
  – These dips are qualitative views of outages
Throughput

- Throughput matches previous estimations in “Sizing Estimates for a Fully Deployed RPKI”
How reliable are the RPKI txns?

- Lots of transient connection errors
- Outages show up as hard failures
  - Descriptions: [http://rpkispider.verisignlabs.com/docs.html#intermittent](http://rpkispider.verisignlabs.com/docs.html#intermittent)
Outages

- Reasons can vary
  - Referential integrity
  - TA rollover
  - PoOO (Plain old Operational Outages)

- Referential integrity failure took one of the 5 repos completely offline
  - Notice was sent to the community after RPKISpider alerted about the problem
Outages (2)

- TA rollovers are an issue that needs attention
  - How can a repo operator *know* when RPs are ready for a rollover

- If a rollover happens before RPs are ready, there is an outage

- One possible direction being investigated: “CoTs and Off-Axis Corroboration:”

- Envisioned interactions with “tightly coupled” BGPSEC could make this *very* problematic
Going forward

• We’ve started using our measurements to codify the global system’s status in a set of metrics

• Sadly, I ran out of time before this preso, or they would be on our page

• The goal is to use the inherent usage model of RPKI to quantify its operational status so alerting, detection, remediation, etc are possible
RPKISpider Usage

• Feel free to lookup prefixes

http://rpkispider.verisignlabs.com/search.html
Thanks