VERISIGN™

Internet Resource Certification and Inter-Domain Routing Security

Eric Osterweil

Who is allowed to do what?

- BGP (the Internet’s inter-domain routing protocol) runs by rumor
  - Participants assert reachability and ``gossip’’ about what they’ve heard from each other

- This has never been overly secure
  - Who is the rightful holder of a resource?
  - Who is allowed to assert reachability for resources?
  - What’s a ``resource!?!?’’

- We’ve always needed resource certification
  - A way to answer: ``who is allowed to do what?’’
- But what is that?

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 resource certification
  - It focuses on routed resources

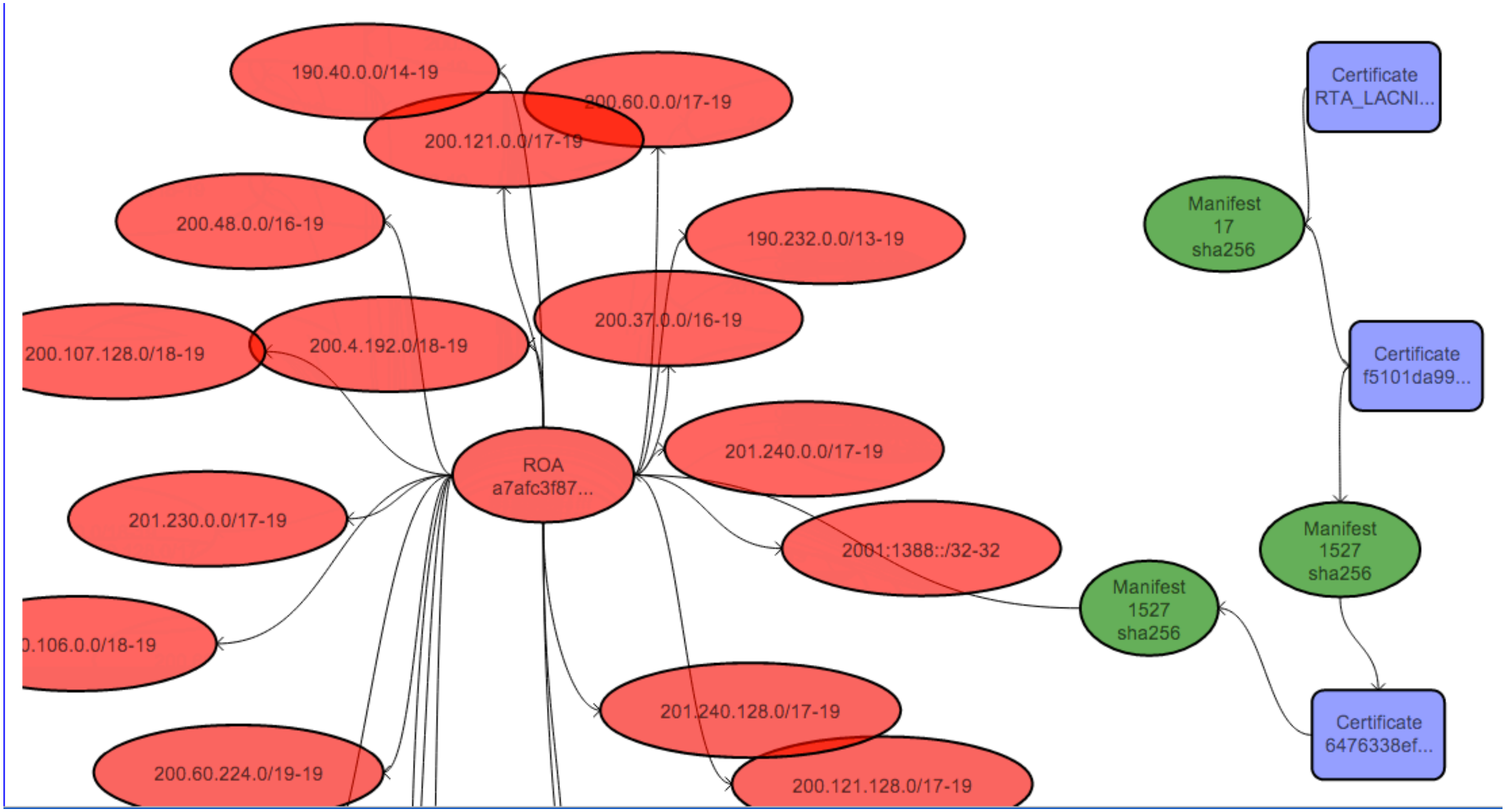
- The envisioned usage for RPKI has morphed from just titleship to routed resource certification
  - BGPSEC uses RPKI to sign and verify BGP updates and a new BGP path attribute

RPKI

- IP addresses are allocated hierarchically
  - IANA allocates addresses to Regional Internet Registries (RIRs) ARIN, RIPE, APNIC, LACNIC, AfriNIC
  - Each RIR allocates further (LIRs, ISPs, etc).
- RPKI envisions that an IANA trust anchor will be used to sign ``objects'' that represent resource allocations it has given to RIRs
  - RIRs would then use signed objects to certify *their* allocations
- So… A prefix may have been allocated from IANA to ARIN to Level(3) to a customer…

VERISIGN™

Allocation



http://rpkispider.verisignlabs.com/

How does RPKI work?

- Trust anchors are certificates
  - Certs point to manifests

- Manifests (Mfts) contain a list of objects that a certificate asserts information about
  - Contains certs, ROAs, etc

- Certs ➔ CRLs, Mfts, [ROAs], [Ghostbuster records]

- ROAs contain an AS number and a set of prefixes

- All objects in the RPKI are verifiable by by certs
  - Manifests, ROAs, and CRLs all have embedded EE certs

VERISIGN™

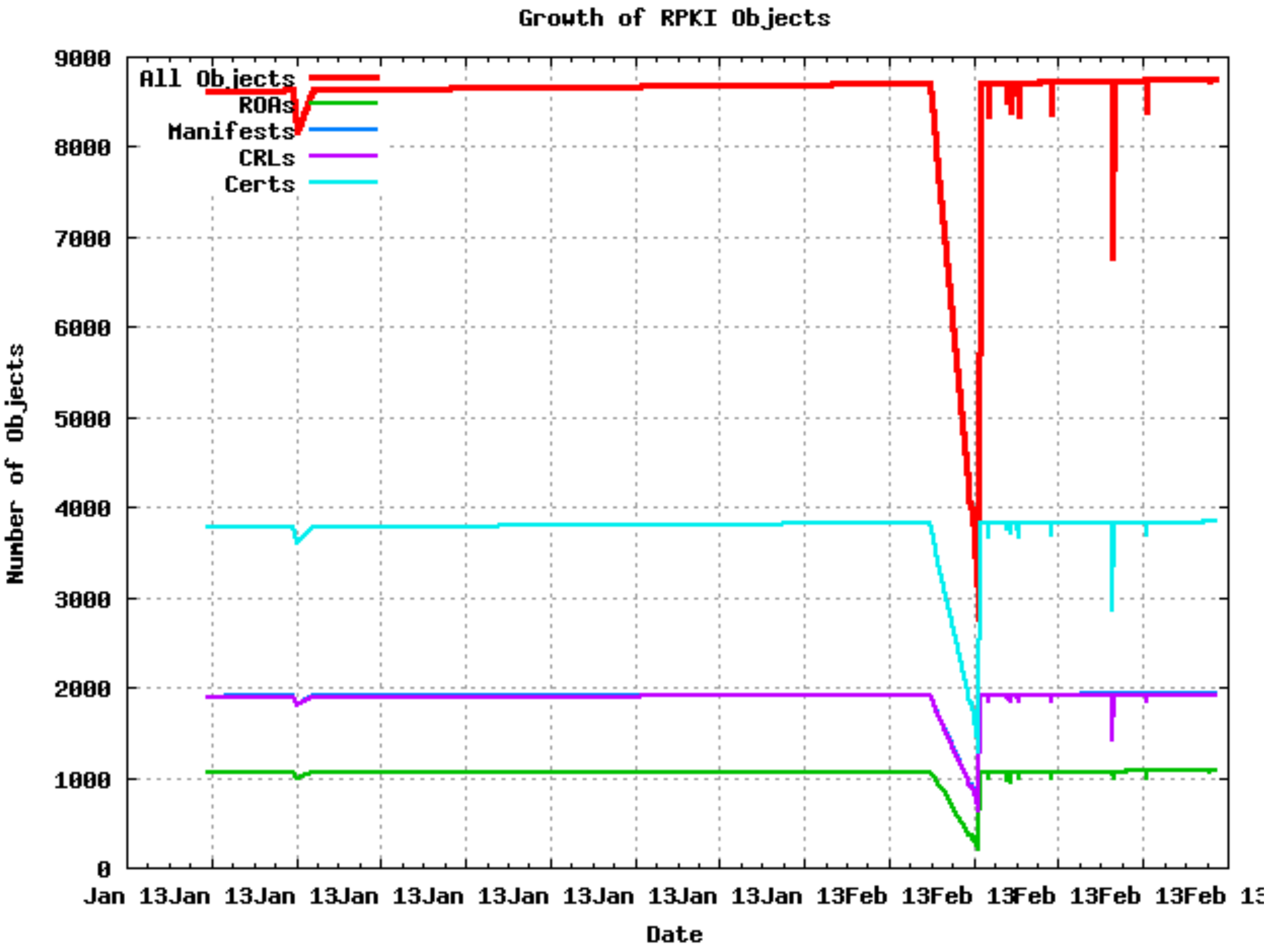
But that’s just the way it’s laid out…

- The entire RPKI is a cryptographic delegation chain
- How many objects are we talking about?
  - We recently did some back of the envelop calculations: 601,337 (Verisign TR #1120005v2):

  http://techreports.verisignlabs.com/tr-lookup.cgi?trid=1120005&rev=2

- However, it is intended to inform BGP’s routing process
  - Routers need keys too… they have to sign/verify updates
  - This would likely balloon object counts to 2,601,377
- eBGP speakers need a way to verify data that they see, so RPKI data needs to wind up near route computation

Where are we *today?*



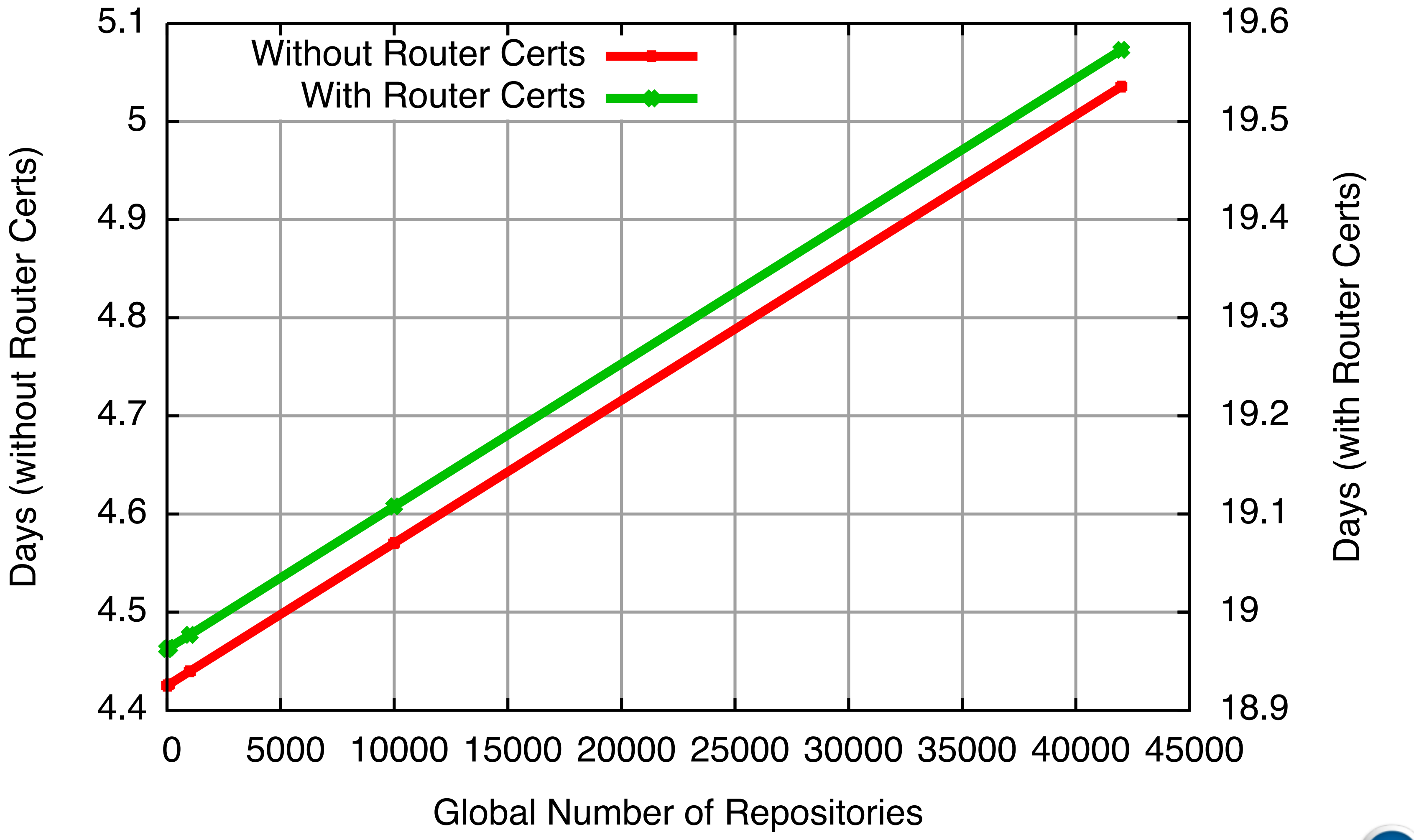
Caching

- RPKI+BGPSEC need routers to have access to the info that RPKI has certified
  - Prefix/origin + router keys
- RPKI caches (run by relying parties) uses rsync
- Our caches must run rsync to all caches for all resource holders in the whole Internet before route verification can happen
  - Currently there are 5 repos, but every resource holder can (and very well may) run their own

Should we be worried?

- RIRs face large challenges converging on a single root
  - So, we have 5 RIRs that each assert 0/0 and can override each other
  - Surgical takedowns are possible (one RIR can surgically affect reachability to another RIR's resources)
- rsync may face scaling challenges…
  - We've already seen rate limiting, connection failures, sub-linear scaling, churn has interrupted, etc…
  - A few high-value targets exists to disrupt routing
- RPKI relies heavily on DNS (many objects are referred to by URIs)

How long might it take to cache from repos?



Worries…

- Today, a routing change can be globally effectuated in minutes
- With RPKI+BGPSEC, this could take days

- Real world example:
  - DDoS providers count on being able to onboard and begin scrubbing customers today
  - Re: Recent financial DDoS attacks, business is goooood…
  - RPKI would mean that it would take significantly longer to onboard
  - ``Sorry Bank of OutOfLuck, we can't protect you for 2 weeks…''
- Research Example:
  - New measurement apparatuses like BGP-mux become infeasible

VERISIGN™

Even so…

- Even if RPKI+BGPSEC gets fully deployed, an entire class of security threat is still 100% unaddressed: Route Leaks

  http://tools.ietf.org/html/draft-grow-simple-leak-attack-bgpsec-no-help-00

- Without a mechanism to learn ``intent,'' issues like route leaks are not addressed
  - Google/Moratel leak, IETF 85 leak through China etc…

- Internet Routing Registries (IRRs) have existed for a long time, and have been used to address this problem since 1995

  http://tools.ietf.org/html/draft-grow-irr-routing-policy-considerations-00

VERISIGN™

What we need is resource certification…

- RPKI is one option, but it doesn't get us all the way there by itself…
- Route leaks happen at an alarming rate
  - Mauch, J., "Detecting Routing Leaks by Counting", October 2007, http://www.nanog.org/meetings/nanog41/presentations/mauch-lightning.pdf
- Some solutions RPKI+IRR Blunk, NANOG 57, RPKI +RPSL sig draft, etc
- DNS has many of the integrity elements that RPKI has and some that it is missing:
  - DNS has data integrity/origin auth + a single root + is extensible to additional Internet resources (beyond routed resources)
  - DANE: s/MIME/TLS/etc
- Even without DNS, RPKI still needs a way to express routing policy
  - Why not use reverse DNS to inform IRRs and build from that?

What’s my [rambling] point?

- There seem to be a copious number of open questions about resource certification
- Attention from the measurement research community would be invaluable
- There’s a lot at stake
  - The FCC is poised to make a recommendation about secure routing and resource certification approaches
  - Vendors are investing heavily
  - etc
- Follow us on Twitter! @RPKIUpdateBot

Thank You

VERISIGN™