Stand Up For Your Routes!
Using the Resource Public Key Infrastructure (RPKI)

Brad Gorman
Senior Product Owner, Routing Security - ARIN
What’s Being Covered Today

• Security of the Early Internet
• The Goal of the RPKI
• Current RPKI Deployment
• RPKI Services and Development
Security of the Early Internet
BGP Routing on the Internet

• BGP enabled the Internet we know today
• Made it easy to establish peering sessions with neighboring networks
• Transitioned from information sharing to a commercial platform
• Scaled beyond where best effort sharing of routing policy was reliable
Routing Policy Specification Language (RPSL)

- RPSL is a standard language used by Internet Service Providers to build security policy on network devices.
- Internet Routing Registry (IRR) is an ecosystem of databases where operators can share information about their policies.
- ARIN authenticates entries in their database, confirming the rightful resource holder created the objects.
- We don’t discourage using a 3rd party IRR for redundancy, however, information cannot be verified.
The Goal of the RPKI
The Goal of the RPKI

• Provide a cryptographically signed method for an Internet number resource holder, allowing them to make an authoritative statement about the origin of a prefix(s) announced to the Internet (Route Origin Authorization, ROA)

• RPKI gives operators another data set to make more informed routing decisions (RPKI Validity State)

• Limit resource holders impact resulting from human error or nefarious activity

• Reduce the overall attack vector for attempted hijacks on the greater Internet
Internet is More Complex Today

AS 200 198.51.100.0

AS 100 192.0.2.0/24

AS 200 198.51.100.0/24
Bad Actors Will Find a Way
RPF in Action

AS 200: 198.51.100.0/24
AS 999: 198.51.100.0/24
RPKI in Action
RPKI in Action

AS 100 192.0.2.0

AS 200 198.51.100.0

AS 999 198.51.100.0

ROA

NANOG
Current RPKI Deployment
RPKI Adoption – Org Participation

- Only **19.5%** of Orgs registered to use ARIN’s RPKI services
  - Hosted – **3,201**
  - Delegated – **80**
  - Repository Service (RPS) – **31**
RPKI ROAs – Covered Prefixes

• Hosted Repository
  • Route Origin Authorizations (ROAs) 53,912
  • Validated ROA Payloads (VRPs*) 65,581

• RPS (Hybrid) Repository
  • ROAs - 1,073
  • VRPs - 2,892

* VRPs identify an IP prefix, a maximum length, and an origin AS number derived from a validated ROA, (verified by ARIN to contain authoritative data).
RPKI Valid Route Announcements

- **28.91%** of Internet routes with ARIN IPv4 resources marked as RPKI Valid*
  - Up **6.5%** year over year
- **47.88%** of Internet routes with ARIN IPv6 resources marked as RPKI Valid*
  - Up **4.2%** year over year

*To be considered RPKI valid there must be a VRP that exactly matches an existing route announcement in the global BGP table.
RPKI Valid IP Resources

45.3% of eligible* ARIN IP resources announced are marked as RPKI valid**

- 508M / 1.12B (eligible)
- 5.0% increase year-over-year

* Resources must be covered by a valid (L)RSA agreement to be eligible for RPKI services at ARIN
** To be considered RPKI valid there must be a VRP that exactly matches an existing route announcement in the global BGP table
We Can Do Better!
RPKI Services and Development
Hosted RPKI Service

- Certificate Authority (CA) managed by ARIN
- Repository and Publication services run by ARIN
- Org creates and maintains their ROAs
- Accessed via ARIN Online portal or the RESTful API

* Easiest to use; Recommended for most organizations just getting started with RPKI. Nearly 98% of ARIN participants use Hosted RPKI.
Delegated RPKI Service

- The organization has more control and independence
- Runs their own CA to manage object signing
- Separation of the publication of cryptographic functions

* Highest responsibility and uptime requirement; only organizations with in-depth knowledge of RPKI and resources to run a Certificate Authority (CA) and a publication server, should select Delegated RPKI.
Repository Publication Service (Hybrid RPKI)

- Maintain control and independence of Delegated RPKI
- Runs their own CA to manage object signing
- Off-load Repository and Publication services to ARIN

* Suggested for organizations that wish to retain cryptographic control, and do not want to maintain the high availability repository and publication functions
Before Getting Started

- IPv4 or IPv6 number resources allocated to your organization by ARIN
- A signed RSA or LRSA (RPKI ToS if needed)
- Autonomous System Number
- Your user account needs to be associated with the org as the Admin, Tech, or Routing Point of Contact (POC)

Keys no longer required to sign ROAs!
Simplified Navigation

- List of all Linked Orgs
- Certification Status
Hosted or Delegated RPKI?

- Formerly a ticketed process
- Required RSD action to complete
One-Step Signup

- Resource certificate is automatically created (covered by RSA/LRSA)
- Ready to create ROAs
Create Your ROA By Fill In The Blank

- No Validity Dates
- No ROA signing keys
ROAs Are Evergreen

- Auto Renewing ROAs!
- All ROAs created in UI switch to auto-renew
Back to Create More ROAs

- Confirm ROA creation
- Direct return to ROA list
- One click to create more ROAs
Stand Up For Your Routes!
Stand Up For your Routes!

• Creating ROAs for your resources benefits more than just you, but also operators who make decisions based on RPKI validity.

• There are documented cases where RPKI has been proven to interrupt hijack attempts before they become impactful.

• More service providers are requiring you create ROAs for your resources before a business relationship is established.

• Ongoing standards work in the IETF is defining new features and use cases for the RPKI.
RPKI Questions For ARIN?

Call the ARIN Helpdesk
• +1.703.227.0660

From the User Dashboard
• Select Ask ARIN
• “Chat with us!”

Routing Security Team
routing.security@arin.net
Thank you