IP Addresses and Routing Security: What ARIN Changes Mean to You

Michael Lambert, Pittsburgh Supercomputing Center/3ROX
KINBERCON 2023
26 April 2023

A few terms

- RIR: Regional Internet Registry
  - A non-profit, member-based organization responsible for administering IP addresses and autonomous system numbers in a region
- ARIN: American Registry for Internet Numbers
  - The RIR serving North America, parts of the Caribbean and some other areas
- RPKI: Resource Public Key Infrastructure
  - A framework aimed at improving routing security in the Internet by cryptographically associating routes with their origin
- ROA: Route Origin Authorization
  - A cryptographically signed object attesting that a given route can come from a particular origin

A few more terms

- RSA: Registration Services Agreement
  - A contract[†] between an organization and ARIN delineating what rights and responsibilities each party has with respect to number resources
- Routing Registry
  - Part of a distributed database containing information such as what routes an organization will be using and what their routing policy is with respect to other networks
  - Some are operated by RIRs
  - Others are operated by ISPs or third parties
- MANRS
  - Mutually Agreed Norms for Routing Security
  - Global initiative to reduce effects of routing threats

[†]I'm not a lawyer; maybe it technically isn't a contract.

What does routing security mean?

- Routes can be announced by someone who shouldn't be announcing them, drawing traffic away from intended destination
  - Sometimes deliberate hijacking
  - More often, operator or equipment error
- Broadly speaking, "routing security" refers to
  - A set of processes, procedures and/or protocols
  - Designed to mitigate the effects of bad route announcements

MANRS

- https://www.manrs.org
- Mainly targets Internet providers, exchange points
- Several steps to improve routing security
  - Prevent propagation of incorrect routing information
    - Filter BGP announcements
  - Facilitate global operational communication and cooperation
    - Register contact information in RIR or PeeringDB
  - Facilitate routing information on a global scale—IRR or RPKI
  - Prevent traffic with spoofed source IP addresses—Filtering
    - Only source traffic with your public addresses
    - BCP 38 (can be question in Campus Cyberinfrastructure proposals)

RPKI and ROAs

- Enable router to check validity of received routes
- Three possible states
  - RPKI Valid: ROA with proper origin exists for received route
  - RPKI Unknown: no ROA exists for received route
  - RPKI Invalid: one or more ROAs exists for received route, but not with this origin
- Many providers reject RPKI Invalid
- AFAIK, RPKI Unknown accepted by everyone

Mechanics of ROAs

- Purpose is to generate cryptographically signed certificate linking route, origin autonomous system
- ~~A little more involved than a simple point and click~~
  - ~~Requires generating and tracking private key~~
  - ~~Pay attention to expiration dates~~
- ARIN releasing new procedures for generating ROAs—they will basically be point-and-click
- Broader community is happy to provide assistance
- Can even delegate through `Routing POC` in ARIN organization record

Further considerations for RPKI/ROA

- At least one provider (that I know of) requiring routes to either be covered by ROA or registered in routing registry run by RIR (ie, ARIN)
  - Many currently use RADB or provider routing registry
  - Seems to be no further push for this
- Push by some to require RPKI for security of routing system
  - Netherlands government has definite plans
- Both ARIN routing registry and RPKI require resources (IP addresses) to be covered by RSA
- Newer resources (including IPv6 space) should already be under agreement (and you're already paying an annual fee to ARIN)
- Legacy resources are a different matter

What are legacy resources?

From the ARIN web site:

“A legacy number resource is an IPv4 address or Autonomous System Number (ASN) that was originally issued to the current registrant by an Internet Registry (InterNIC or its predecessors) prior to the inception of ARIN on 22 December 1997.”

What services do we get without an RSA?

Service	Provided by ARIN?
Maintain unique registration in Whois/RDAP	Yes
Update and manage publicly available data in Whois/RDAP	Yes
Manage reverse DNS delegations	Yes
Maintenance of registry records (ARIN Online)	Yes
DNS Security (DNSSEC) access	Yes
Resource Public Key Infrastructure (RPKI) access	No
Internet Routing Registry (IRR) access	No
Transfer address space	No

From www.arin.net

Why is this important now?

- ARIN charges annual fee for resources under an RSA
  - Based on size of allocation: $250 for /24; $4,000 for /16
- Cap on fee for legacy resources
  - $175 this year
  - Increases by $25 per year
  - Up to full rate for resources (over 150 years for a /16)
  - If you already have some resources under RSA, **might not** pay more
- Cap is going away for legacy resources not under RSA
  - Cutoff is 31 December 2023
  - Full rate for anything brought under RSA after that

Whom behind KINBER does this affect?

Entity	Full Fee	Capped Fee	Savings	Networks
Bloomsburg University	$4,000	$175	$3,825	148.137.0.0/16
Comm Coll of Allegheny Co	$4,000	$175	$3,825	162.51.0.0/16
Duquesne University	$8,000	$175	$7,825	165.190.0.0/16 192.135.213.0/24 192.135.79.0/24
East Stroudsburg University	$2,000	$175	$1,825	192.147.113.0/24 192.148.218.0/24 192.153.187.0/24 206.225.96.0/19
Edinboro University	$4,000	$175	$3,825	147.64.0.0/16

Courtesy of Steven Wallace, Internet2

Whom behind KINBER does this affect?

3ROX
THREE RIVERS OPTICAL EXCHANGE

Entity	Full Fee	Capped Fee	Savings	Networks
Franklin and Marshall College	$4,000	$175	$3,825	155.68.0.0/16
Geisinger System Services	$4,000	$175	$3,825	159.240.0.0/16
Harrisburg Area Community College	$250	$175	$75	199.254.212.0/24
Kutztown University	$4,000	$175	$3,825	156.12.0.0/16
Lafayette College	$8,000	$175	$7,825	139.147.0.0/16 192.48.95.0/24
Lehigh University	$4,000	$175	$3,825	128.180.0.0/16

Courtesy of Steven Wallace, Internet2

Whom behind KINBER does this affect?

Entity	Full Fee	Capped Fee	Savings	Networks
Lock Haven University	$4,000	$175	$3,825	151.161.0.0/16
Millersville University	$8,000	$175	$7,825	166.66.0.0/16 192.206.29.0/24
PASSHE	$2,000	$175	$1,875	204.235.144.0/20 204.235.162.0/23
Shippensburg University	$4,000	$175	$3,825	157.160.0.0/16
Slippery Rock University	$2,000	$175	$1,825	192.148.234.0/24 205.149.64.0/19

Courtesy of Steven Wallace, Internet2

Whom behind KINBER does this affect?

3ROX
THREE RIVERS OPTICAL EXCHANGE

Entity	Full Fee	Capped Fee	Savings	Networks
Hershey Medical Center	$4,000	$175	$3,825	150.231.0.0/16
Villanova University	$4,000	$175	$7,825	153.104.0.0/16

Courtesy of Steven Wallace, Internet2

Summarizing finances

- Annual impact to KINBER community of registering routes
  - Full ARIN rate: $74,250
  - Capped rate: $3,150
  - Savings: $71,100
- Maybe more important
  - 940,800 IPv4 addresses not covered
  - Current open-market rate is $38-40 per address
  - That's about $36 million in unprotected assets[†] just among KINBER members
  - Over $1 billion through entire US R&E community

[†]These addresses may or may not really be assets.

What does all this mean?

- What if we just don't put blocks under RSA?
  - Won't pay fees (at least under current policies)
  - But IPv4 space **might not** be routable in Internet
  - Can't transfer IP addresses
  - Can't do RPKI for routing security
    - Hijacks are possible
    - Mistakes are more likely
- Good time to consider RSA
  - Starting point is https://www.arin.net/resources/guide/legacy/
  - Word of warning: redlining generally not accepted
  - Exceptions for public entities with statutory requirements for indemnification, arbitration, etc
  - And you might look at https://youtu.be/4l1zFRgDyB8, presented by Steve Wallace of Internet2

3ROX
THREE RIVERS OPTICAL EXCHANGE

Questions?