RPKI Tutorial

MANRS RPKI Week
July 2022

Massimiliano Stucchi
stucchi@isoc.org
Agenda

Introduction

ROAs
- **Demo:** Create ROAs

Deploying RPKI Validators
- **Demo:** Running Validators

Validation
- **Demo:** Setting up BGP Origin Validation
- **Demo:** Discarding BGP Invalids
Routing on the Internet

B: “I have 213.x.x.x”
A: “I have 193.x.x.x”

Routing table
213.x.x.x = B

Routing table
193.x.x.x = A

Network A
193.x.x.x

Network B
213.x.x.x

Can I trust B?

Is A correct?

“BGP Protocol”
How can you have secure routing?

Network A
193.x.x.x

Routing table
213.x.x.x = B

Network B
213.x.x.x

Routing table
193.x.x.x = A

B: “I have 213.x.x.x”

A: “I have 193.x.x.x”

“Internet Routing Registry”

RIPE Database

Can I trust B?

Is A correct?
Problem Statement

• Some IRR data cannot be fully trusted
  - Accuracy
  - Incomplete data
  - Lack of maintenance

• Third party databases are widely used
  - No verification of who holds IPs/ASNs
A Short History

• Operated since 2008 by all RIRs
  - Community-driven standardisation (IETF)

• Adds crypto-security to IP addresses and ASNs
  - Provides data you can trust
RPKI Chain of Trust

**ALL** Resources

- public key
- signature

Root's *private* key
RPKI Chain of Trust

LIR’s Resources
- public key
- signature

Root’s private key
RPKI Chain of Trust

Root’s private key

ALL Resources
- public key
- signature

LIR’s Resources
- public key
- signature
Resource Public Key Infrastructure

Ties IP addresses and ASNs to public keys

Follows the hierarchy of the registries

Authorised statements from resource holders
“ASN X is authorised to announce my Prefix Y”
Signed, holder of Y
ROAs
Elements of RPKI

- Signing
  - Create your ROAs

- Validating
  - Verifying others
Elements of RPKI

- Signing
  - Create your ROAs

- Validating
  - Verifying others
What is a ROA?

An **authorised statement** from a resource holder
What is a ROA?

• LIRs can create a ROA for their resources

• Multiple ROAs can exist for the same prefix
  - With different origin/maxlength

• ROAs can overlap
What is in a ROA?

- **Prefix**: The network for which you are creating the ROA
- **Origin ASN**: The ASN supposed to originate the BGP Announcement
- **Max Length**: The maximum prefix length that ROA is authorised to advertise
What is max-length?
How should we use max-length?

You created a single ROA authorising the entire /22
How should we use max-length?

Create ROAs for BGP announcements only

Max length

/23

/22

/23

/24

Invalid

Attacker's announcement
ROA Signature

Prefix is authorised to be announced by AS Number

LIR’s private key

ROA signature
RPKI Chain of Trust

- **ALL Resources**:
  - Public key
  - Signature

- **LIR’s Resources**:
  - Public key
  - Signature

- **ROA**
  - Signature
RPKI Certificate Structure

Certificate hierarchy follows allocation hierarchy

- ARIN
- APNIC
- RIPE
- LACNIC
- AFRINIC

Member

ROA

ROA

ROA
Hosted or Delegated RPKI

 RIPE

 Member
 ROA
 ROA
 Member-X CA

 Member
 ROA
 ROA
 Member-Y CA

 RIPE NCC Hosted System

 Member
 ROA
Hosted RPKI

• RIR hosts a CA and signs all ROAs

• Automate signing and key rollovers

• Allows you focus on creating and publishing ROAs
Delegated RPKI

- Run your own Certificate Authority software
  - Dragon Research Labs, RPKI Toolkit
  - NLnetlabs, Krill

- Setup connection with RIR CA

- Generate your LIR certificate and get it signed by parent CA
Certifying PI Resources

Requested and managed by PI End User or by Sponsoring LIR

1. Complete the wizard successfully

2. Login to https://my.ripe.net and request a certificate
   - Sign in with your RIPE NCC Access account

3. Manage your ROAs
Creating ROAs

Demo on the RIPE NCC LIR Portal
RPKI Validators
Elements of RPKI

Signing

Create your ROAs

Validating

Verifying others
RPKI Validators

• Software that creates a local “validated cache” with all the valid ROAs
  - Downloads the RPKI repository from the RIRs
  - Validates the chain of trust of all the ROAs and associated CAs
  - Talks to routers using the RPKI-RTR Protocol
Trust Anchor Locator (TAL)

- Location of RIR repositories
- Root's public key

List of ROAs

RIPE NCC
ARIN
APNIC
LACNIC
AFRINIC

Repository
Repository
Repository
Repository
Repository

TAL
TAL
TAL
TAL
TAL

Validator

Certificates
Relying Party
Relying Party

BETTER ROUTING DECISIONS

<table>
<thead>
<tr>
<th>AS</th>
<th>CIDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS111</td>
<td>10.0.8.0/22</td>
</tr>
<tr>
<td>AS222</td>
<td>10.0.6.0/24</td>
</tr>
<tr>
<td>AS333</td>
<td>10.4.16.0/20</td>
</tr>
<tr>
<td>AS111</td>
<td>10.0.12.0/22</td>
</tr>
<tr>
<td>AS111</td>
<td>10.0.16.0/22</td>
</tr>
<tr>
<td>AS111</td>
<td>10.0.20.0/22</td>
</tr>
</tbody>
</table>
RPKI Validator Options

- **Routinator**
  - Built with Rust, built by NLNetlabs

- **rpki-client**
  - Part of OpenBSD project, written in C

- **OctoRPKI**
  - Cloudflare’s Relying Party software, written in Go

- **FORT**
  - Open source RPKI validator, Written in C
Configuring and Running Validators

Demo
How to Configure Validators

Run at least two validators
  • Routinator
  • FORT

Configure the correct TALs
  • They have already been downloaded
  • ARIN TAL needs to be “acknowledged” separately
Start Routinator

On the Server:

```
routinator server --rtr 100.64.1.1:3323
```

- TAL directory is **missing!**
- We need to initialize via **init command!**
[root@server1 ~]# routinator server --rtr 100.64.1.1:3323
Missing TAL directory /root/.rpki-cache/tals.
You may have to initialize it via 'routinator init'.

[root@server1 ~]# routinator init
Before we can install the ARIN TAL, you must have read and agree to the ARIN Relying Party Agreement (RPA).
It is available at

If you agree to the RPA, please run the command again with the --accept-arin-rpa option.

[root@server1 ~]# routinator init --accept-arin-rpa
Created local repository directory /root/.rpki-cache/repository
Installed 5 TALs in /root/.rpki-cache/tals
Start Routinator

On the Server:

```bash
routinator server --rtr 100.64.1.1:3323
```

Check if it's running

```bash
ps aux | grep routinator
```
Start FORT validator

On the Server:

```
systemctl start fort
```

Check if it is running and the logs (exit with ctrl-c):

```
systemctl status fort
journalctl -u fort
```
Start FORT validator

On the Server:

```
fort --init-tals --tal=/etc/fort/tal
```

```
[root@server1 ~]# fort --init-tals --tal=/etc/fort/tal
Please download and read ARIN Relying Party Agreement (RPA) from https://www.arin.net/resources/manage/rpki/rpa.pdf. Once you've read it and if you agree ARIN RPA, type 'yes' to proceed with ARIN's TAL download:

yes
Successfully fetched '/etc/fort/tal/arin.tal'!
Successfully fetched '/etc/fort/tal/apnic.tal'!
Successfully fetched '/etc/fort/tal/afrinic.tal'!
Successfully fetched '/etc/fort/tal/ripe.tal'!
Successfully fetched '/etc/fort/tal/lacnic.tal'!
```
Validation (ROV)
Validation

ROA Validation

BGP Origin Validation

RIR Repository
- ROAs
- Certificates

Validator

Rsync/RRDP

RPKI-RTR

Validated Cache

AS 100

AS 200
ROA Validation

ALL Resources
- public key
- signature

LIR’s Resources
- public key
- signature

ROA
- signature
BGP Prefix Origin Validation-RFC6811

[Diagram showing ROAs and validation process]

ROAs

AS 100

AS 200

10.0.0.0/22

10.0.0.0/24

ROA
AS100 10.0.0.0/22

VALIDATOR

RPKI-RTR

46
RPKI Validation States

ROA Validation

- **VALID**
- **INVALID**

BGP Origin Validation

- **VALID**
- **INVALID**
- **NOT FOUND**
Local Changes to ROA DB (using SLURM)

ROAs

VALIDATOR

ROA
AS100 10.0.0.0/22

RPKI-RTR

AS 100

10.0.0.0/24
Local Changes to ROA DB (using SLURM)
Cisco Origin Validation configuration

(config)# conf t
(config)# router bgp $ASN
(config-router)# bgp rpki server tcp 100.64.1.1 port 8323 refresh 300
(config-router)# bgp rpki server tcp 100.64.1.1 port 3323 refresh 300
Cisco Origin Validation configuration

(config-router)# route-map rpki-accept permit 10
(route-map)# match rpki valid
(route-map)# set local-preference 100
(route-map)# route-map rpki-accept permit 20
(route-map)# match rpki not-found
(route-map)# set local-preference 80
Cisco Origin Validation configuration

(config)# router bgp $ASN
(config)# address-family ipv4
(config)# neighbor 192.168.1.254 route-map rpki-accept in
(config)# address-family ipv6
(config)# neighbor 2002:eeee:ffff::a route-map rpki-accept in
Juniper Origin Validation configuration

```plaintext
routing-options {
  autonomous-system 64511;
  validation {
    group rpki-validator {
      session 100.64.1.1 {
        refresh-time 120;
        hold-time 180;
        port 8282;
        local-address 100.64.1.2;
      }
    }
  }
}
```
policy-statement send-direct {
  from protocol direct;
  then accept;}
policy-statement validation {
  term valid {
    from {
      protocol bgp;
      validation-database valid; }
    then {
      local-preference 110;
      validation-state valid;
      community add origin-validation-state-valid;
      accept;
    }}}
Juniper Origin Validation configuration

term invalid {
  from {
    protocol bgp;
    validation-database invalid;
  }
  then {
    local-preference 90;
    validation-state invalid;
    community add origin-validation-state-invalid;
    accept;
  }
}
Juniper Origin Validation configuration

term **unknown** {
    from protocol bgp;
    then {
        validation-state **unknown**;
        community add origin-validation-state-unknown;
        accept;
    }
}
Route Origin Validation (ROV)

Demo
Demo Setup

BGP Announcements
AS58280 45.129.224.0/22
AS58280 45.129.226.0/24

Prefix is supposedly invalid
Validators

There are instances of Fort and Routinator running

We now need to configure them on our router

```
rpki
rpki cache 103.162.143.28 3323 preference 1
rpki cache 103.162.143.29 8323 preference 2
```
Validators

And then we can check if it worked

Show rpki prefix-table
Configuring ROV

First step is to create a route-map

```
route-map rpki permit 20
  match rpki notfound
  set local-preference 100
!
route-map rpki permit 30
  match rpki valid
  set local-preference 120
```
And then we apply it to the bgp neighbor

```
router bgp 101
neighbor 123.123.123.0 route-map rpki in
```

... and 45.129.226.0/24 should disappear from our table
Other actions

• You could tag the validated routes with a specific community
  … and the not found ones with another community
Origin Validation Check

• Go with your browser to

http://www.ripe.net/s/rpki-test

• And check if your network applies Origin Validation
Wrapping up
Some suggestions

• Run multiple validators, both in type and location

• Monitor them
  
  Check that the serial number keeps increasing
BGP Alerter

• You can use it to monitor your announcements

  • https://github.com/nttgin/BGPalerter

  • Very quick setup, monitors changes in your announcements based on RIS data
MANRS Training Tutorials

6 training tutorials based on information in the Implementation Guide.

A test at the end of each tutorial.

About to begin training moderators for online classes (43 applications received!)

https://www.manrs.org/tutorials
MANRS Hands-on Lab

The prototype lab is ready, finalising the production version.

- Cisco
- Juniper
- Mikrotik

Can be used as a standalone lab or as a final exam
Join MANRS

Visit https://www.manrs.org

• Fill out the sign up form with as much detail as possible.
• We may ask questions and request tests

Get Involved in the Community

• Participants support the initiative and implement the actions in their own networks and encouraging MANRS adoption
• Participants are engaged in substantive activities – developing MANRS requirements and guidance, assisting with capacity and awareness building activities
Questions ?

stucchi@isoc.org
@stucchimax