RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

Taejoong (Tijay) Chung§, Emile Aben†, Tim Bruijnzeels‡,
Balakrishnan Chandrasekaran△, David Choffnes*, Dave Levin†,
Bruce Maggs°♦, Alan Mislove*, Roland van Rijswijk-Deij‡±,
John Rula*, Nick Sullivan*

§Rochester Institute of Technology, †RIPE NCC, ‡NLNetLabs,
△Max Planck Institute for Informatics, *Northeastern University, †University of Maryland,
°Duke University, ±University of Twente, ♦Akamai Technologies, *Cloudflare
RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins
Resource PKI
(Public Key Infrastructure)

- Public Key Infrastructure framework designed to secure Internet’s routing structure; specifically BGP (developed starting in 2008)
RPKI: How it works?

What does a resource owner need to do to protect their IP prefixes?

How can a router verify it using RPKI?

Router

BGP announcement

Owner

RIT

AS 4385
129.21.0.0/16
Certificate

RPKI Structure

MaxLength

Validated ROA Payload (VRP)

5

RIT
129.21.0.0/16
AS 4385

Certificate

ROA

Route Origin Authorization

129.21.0.0/20, AS 4385
129.21.1.0/20, AS 4385

\cdot

129.21.240.0/20, AS 4385

129.21.0.0/16-20, AS 4385

MaxLength

AS 4385

129.21.0.0/16
Regional Internet Registries

Certificate

RPKI Structure

MaxLength

{ 129.21.0.0/20, AS 4385
  129.21.1.0/20, AS 4385
  129.21.240.0/20, AS 4385
  129.21.0.0/16-20, AS 4385
}

Route Origin Authorization

ROA

Certificate

LIRs (e.g., ISP)

Sign

129.21.0.0/16
AS 4385

Validated ROA Payload (VRP)

MaxLength
RPKI: How it works?

What does an resource owner needs to do to protect their IP prefixes?

Router

BGP announcement

RIT  AS 4385
129.21.0.0/16

Owner

How can a router verify BGP announcements using RPKI?
RPKI: How it works?
Validation process: Valid
RPKI: How it works?
Validation process: Valid (w/ MaxLength)

Prefix-to-AS Mapping Database

1.1.0.0/16 AS 111
2.0.0.0/8-16 AS 222
3.3.0.0/16 AS 333
4.4.4.0/24 AS 444

BGP announcement

2.24.0.0/16 AS 222
RPKI: How it works?
Validation process: Invalid (too-specific)

Prefix-to-AS Mapping Database

- 1.1.0.0/16 AS 111
- 2.0.0.0/8-16 AS 222
- 3.3.0.0/16 AS 333
- 4.4.4.0/24 AS 444

BGP announcement

3.3.3.0/24 AS 333

Covered, but the announcement is too specific

Router
RPKI: How it works?
Validation process: Invalid (wrong ASN)

Prefix-to-AS Mapping Database

- 1.1.0.0/16 AS 111
- 2.0.0.0/8-16 AS 222
- 3.3.0.0/16 AS 333
- 4.4.4.0/24 AS 444

BGP announcement

4.4.4.0/24 AS 555

Router

IP prefix is matched, but the ASN is different.
RPKI: How it works?
Validation process: Unknown (Uncovered)

Prefix-to-AS Mapping Database
- 1.1.0.0/16 AS 111
- 2.0.0.0/8-16 AS 222
- 3.3.0.0/16 AS 333
- 4.4.4.0/24 AS 555

Router

BGP announcement
- 5.5.0.0/16 AS 555

Uncovered, thus unknown
RPKI: How it works?
Validation Process

There is a VRP that “covers” IP prefix

The ASN of the VRP and the ASN in the BGP are identical?

There is a VRP that matches IP prefix (using MaxLength, if exists)
Alright, so in this talk..
RPKI is Coming of Age
A Longitudinal Study of RPKI Deployment and Invalid Route Origins

Why do we study RPKI?

It is relatively new
It works differently
It is easy to deploy
# Datasets (1)
## RPKI Objects

<table>
<thead>
<tr>
<th></th>
<th>Measurement Period*</th>
<th>VRPs (from the latest snapshot)</th>
<th></th>
<th>Percent of ASes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>APNIC</td>
<td>2011-01 ~ 2019-02</td>
<td>14,025</td>
<td>14,025</td>
<td>8.14%</td>
</tr>
<tr>
<td>LACNIC</td>
<td>2011-01 ~ 2019-02</td>
<td>4,510</td>
<td>4,510</td>
<td>9.33%</td>
</tr>
<tr>
<td>RIPECC</td>
<td>2011-01 ~ 2019-02</td>
<td>40,830</td>
<td>40,830</td>
<td>16.04%</td>
</tr>
<tr>
<td>ARIN</td>
<td>2012-09 ~ 2019-02</td>
<td>4,575</td>
<td>4,575</td>
<td>1.47%</td>
</tr>
<tr>
<td>AFRINIC</td>
<td>2011-01 ~ 2019-02</td>
<td>176</td>
<td>176</td>
<td>3.30%</td>
</tr>
</tbody>
</table>

*https://ftp.ripe.net/rpki*
A general increasing trend in adoption of RPKI!

It varies significantly between RIRs:
1.38% (ARIN) ~ 15.11% (RIPENCC) of ASes and
2.7% (AFRINIC) ~ 30.6% (RIPENCC) of IPv4
addresses are authorized by VRPs

* AS4775, AS10091, AS9299
## Datasets (2)
### BGP Announcements

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Measurement Period</th>
<th># of VPs</th>
<th># of Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE-RIS</td>
<td>2011-01 ~ 2018-12</td>
<td>24</td>
<td>905K</td>
</tr>
<tr>
<td>RouteViews</td>
<td>2011-01 ~ 2018-12</td>
<td>23</td>
<td>958K</td>
</tr>
<tr>
<td>Akamai</td>
<td>2017-01 ~ 2018-12</td>
<td>3,300</td>
<td>1.94M</td>
</tr>
</tbody>
</table>

More than 46 Billion BGP announcements
Deployment: BGP announcements w/ RPKI

RPKI-enabled BGP announcements are consistently increasing.
RPKI validation over BGP announcements

- 46.8 B
  - 43 B (91.9%) (unknown)
  - 3.5 B (90.4%)
  - 344 M (9.6%)
- 3.8 B (8.1%)
  - Covered
During 2011, 48.92% covered announcements were invalid; 27.47% of invalid were due to announced IP prefixes being covered, but not matched with VRPs.
Then, why are they invalid?

- There is a VRP that “covers” IP prefix
- The ASN of the VRP and the ASN in the BGP are identical?
- There is a VRP that matches IP prefix (using MaxLength, if exists)

? × ×
Then, why are they invalid?

There is a VRP that “covers” IP prefix

The ASN of the VRP and the ASN in the BGP are identical?

There is a VRP that matches IP prefix (using MaxLength, if exists)

Potential Reasons:
- Malicious hijacking attacks?
- Wrong ASN

Potential Reasons:
- Misunderstanding of ROAs (VRPs) of network operators*
- Stale ROAs
- ...

Too specific vs. Wrong ASNs

![Graphs showing the number of unique invalid advertisements over time for Akamai, RIPE-RIS, and Routeviews. The graphs compare Too Specific and Wrong ASNs.]
Too specific vs. Wrong ASNs

**AS 5089 (Virgin Media Limited)**
- On April 16, 2018, 3,200 IP prefixes are more specific than the VRPs; none of them specified MaxLength.

**AS 12322 (Free SAS)**
- 6 ROAs for 7,671 (96.0%) IP prefixes are more specific than the VRPs (w/o MaxLength).
- 8,800 IP prefixes went invalid failing to specify a proper value for MaxLength.

---

**Graphs:**
- **Akamai**: Too Specific
- **RIPE-RIS**: Too Specific
- **Routeviews**: Too Specific

**Dates:**
- **January 21, 2012**: 6 ROAs for 7,671 (96.0%) IP prefixes are more specific than the VRPs (w/o MaxLength).
- **January 22, 2012**: Added the MaxLength to include more specific IP prefixes.
- **October 23, 2018**: 8,800 IP prefixes went invalid failing to specify a proper value for MaxLength.
Too-specific and MaxLength attribute

The use of MaxLength has been decreasing

52.3% of the valid IP prefixes are validated through VRPs with the MaxLength attribute

92% of too-specific announcements are due to VRPs that do not have the MaxLength attribute
The number of BGP announcements having a wrong ASN

<table>
<thead>
<tr>
<th>Date</th>
<th>Akamai</th>
<th>RIPE-RIS</th>
<th>Routeviews</th>
<th>Provider—Customer Relationship</th>
<th>DDoS Protection</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>An AS can sub-allocate part of its IP prefixes to its customer</td>
<td>Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)</td>
<td>We don’t know, but it could be malicious (e.g., hijacking)</td>
</tr>
<tr>
<td>2012</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Wrong ASN
Wrong ASN:  
Same ISP

<table>
<thead>
<tr>
<th>Same ISP</th>
<th>Two different ASNs are managed by the same operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider—Customer Relationship</td>
<td>An AS can sub-allocate part of its IP prefixes to its customer</td>
</tr>
<tr>
<td>DDoS Protection</td>
<td>Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)</td>
</tr>
<tr>
<td>Other</td>
<td>We don’t know, but it could be malicious (e.g., hijacking)</td>
</tr>
</tbody>
</table>

Telmex Columbia S.A. manages two ASes (AS 10620, 14080)
AS 10620 announced 1,500 prefixes supposed to be from AS 14080 for 9 months
Wrong ASN:
Provider — Customer Relationship

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same ISP</td>
<td>Two different ASNs are managed by the same operator</td>
</tr>
<tr>
<td>Provider—Customer</td>
<td>An AS can sub-allocate part of its IP prefixes to its customer</td>
</tr>
<tr>
<td>Relationship</td>
<td>DDoS Protection</td>
</tr>
<tr>
<td></td>
<td>Origin ASes may outsource “scrubbing” of their traffic by using traffic</td>
</tr>
<tr>
<td></td>
<td>diversion to a DDoS protection service (DPS)</td>
</tr>
<tr>
<td>Other</td>
<td>We don’t know, but it could be malicious (e.g., hijacking)</td>
</tr>
</tbody>
</table>

P-C and C-P are quite prevalent; mainly due to providers that have not updated after leasing to the IP prefixes customers (up to 89.45%) such as AS 6128 (CableVision Systems) allocating to 9 different ASes.
Wrong ASN: DDoS Protection

We rarely see announcements from DDoS protection services
AS 26415 (Verisign) announced 6 IP prefixes of AS 13285 (TalkTalk)
AS 19905 (Neustar) announced 1 IP prefix of AS 21599

<table>
<thead>
<tr>
<th>Same ISP</th>
<th>Two different ASNs are managed by the same operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider—Customer Relationship</td>
<td>An AS can sub-allocate part of its IP prefixes to its customer</td>
</tr>
<tr>
<td>DDoS Protection</td>
<td>Origin ASes may outsource “scrubbing” of their traffic by using traffic diversion to a DDoS protection service (DPS)</td>
</tr>
<tr>
<td>Other</td>
<td>We don’t know, but it could be malicious (e.g., hijacking)</td>
</tr>
</tbody>
</table>

We rarely see announcements from DDoS protection services
AS 26415 (Verisign) announced 6 IP prefixes of AS 13285 (TalkTalk)
AS 19905 (Neustar) announced 1 IP prefix of AS 21599
Wrong ASNs:
The others (possibly suspicious)

(1) AS 37468 (Angola Cables) announced more than 2,500 IP prefixes owned by 82 ASes on May 11, 2018 and **15,000** IP prefixes owned by 1,554 ASes on July 19, 2018

(2) Targeted attack: AS 55649 (a private ISP in Hong Kong) announced 1,091 IP prefixes owned by 12 ASes, 10 of which are in China on February 28, 2018

(3) Targeted attack: 401 IP prefixes owned by AS 27738 (Ecuadortelecom S.A.) are announced by 743 ASes on January 7, 2018?
Case-study: BGPStream

Hijack Reports from BGPStream

2,361 IPv4 Reports

2,082 IP prefixes are unknown to RPKI

279 IP prefixes are covered by at least one VRPs

263 (94.27%) are in our “unknown” category

6 (2.15%) in the same ISP

10 (3.58%) provider and customer relationship

0 DDoS Protection ASes
Conclusion and Discussion

• RPKI has been widely deployed

  • RPKI Objects: 2.7% (AFRINIC) ~ 30.6% (RIPE NCC) of the total IPv4 space is covered

  • BGP announcements: 8.1% of BGP announcements are covered

• 2~4 % of (verifiable) BGP announcements are invalid!

  • Too specific announcements

  • Wrong ASNs

• Open Question: how can we identify hijacking attempt with high confidence?
Thanks!

https://rpki-study.github.io
(and https://securePKI.org)

Datasets, code, figures, and instructions are available!

tjc@cs.rit.edu