The complex reality of protecting BGP

Quantifying the impact of RPKI validation in ISPs and IXPs

Niklas Vogel, and Haya Shulman

German National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT
Goethe University Frankfurt
Motivation BGP and RPKI
The inherent Hijack-Problem in BGP

Attackers can hijack IP traffic
Preventing Hijacks with the RPKI

RPKI prevents Hijacks
Preventing Hijacks with the RPKI

Publication Section
Preventing Hijacks with the RPKI

Systems publish ROAS
How many Systems publish ROAs?

Adaption of RPKI is increasing

Preventing Hijacks with the RPKI

Enforcement Section
Preventing Hijacks with the RPKI

VRPs
AS1, 1.0.0.0/8
AS1, 2.0.0.0/8
AS1, 3.0.0.0/8
AS2, 6.0.0.0/8

Routers enforce ROV
How many Systems enforce ROV?

<table>
<thead>
<tr>
<th>Project Name</th>
<th>Year</th>
<th>ROV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloudflare [1]</td>
<td>2023</td>
<td>30%</td>
</tr>
<tr>
<td>APNIC [2]</td>
<td>2023</td>
<td>29.3%</td>
</tr>
<tr>
<td>Rodday et al. [3]</td>
<td>2021</td>
<td>0.6%</td>
</tr>
</tbody>
</table>

30% of Systems enforce ROV

Open Questions answered in this Talk

- How many systems are (just) upstream protected?
- Does ROV-enforcement differ by AS-Type?
- What role do IXP Routeservers play in ROV?
- How well is today’s Internet protected against hijacks?
Measuring ROV Deployment
How to measure ROV Deployment?

- How to identify if a system enforces ROV?
  - => Announce hijacks

- How to identify upstream protection?
  - => Measure paths

- How to quantify role of IXPs?
  - => Use IP paths instead of AS paths (Traceroute)
How to measure ROV Deployment?

- Setup: No RPKI

Both prefixes are announced by both ASes
How to measure ROV Deployment?

- Setup: No RPKI
How to measure ROV Deployment?

- Setup: No RPKI
How to measure ROV Deployment?

- Setup: No RPKI

Prefixes routed identically

I own Prefix 1!
I own Prefix 2!
How to measure ROV Deployment?

- With RPKI

```
1 <-> 2 <-> 3
P_1  P_2
```

```
O_1
I own Prefix 1!
I own Prefix 2!

O_2
I own Prefix 1!
I own Prefix 2!
```
How to measure ROV Deployment?

- With RPKI
How to measure ROV Deployment?

- With RPKI

Prefixes routed identically
No ROV in 1, 2, 3
How to measure ROV Deployment?

- With ROV

AS3 enforces ROV

I own Prefix 1!
I own Prefix 2!

O₁

O₂

P₁

P₂
How to measure ROV Deployment?

- With ROV

![Diagram showing the flow of ROV deployment with nodes 1, 2, 3, and two paths P₁ and P₂, and event nodes O₁ and O₂ with messages indicating ownership of prefixes 1 and 2.]

I own Prefix 1!
I own Prefix 2!
I own Prefix 1!
I own Prefix 2!
How to measure ROV Deployment?

- With ROV

Prefix routing diverges
How to measure ROV Deployment?

- With ROV

Divergence Point enforces ROV
How to classify ROV Deployments?

- No strict Enforcement

<table>
<thead>
<tr>
<th>Category</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
</table>

Invalid Paths

Valid Paths
How to classify ROV Deployments?

- Passive Protection

<table>
<thead>
<tr>
<th>Category</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
</table>

**Invalid Paths**

**Valid Paths**
How to classify ROV Deployments?

- **Active Protection**

<table>
<thead>
<tr>
<th>Category</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
</table>

**Invalid Paths**

<table>
<thead>
<tr>
<th>Divergence Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Invalid Paths</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Divergence Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Valid Paths</td>
</tr>
</tbody>
</table>

**Table:**

- **Category**
  - 1: Negative Evidence
  - 2: Weak depref.
  - 3: Strong depref.
  - 4: No neg. Evidence
  - 5: Upstream protected
  - 6: Some pos. Evidence
  - 7: Strong pos. Evidence
Measurement Results
### Results ROV Enforcement

<table>
<thead>
<tr>
<th>Category</th>
<th>1 - 3</th>
<th>4 - 5</th>
<th>6 - 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>No strict Enforcement</td>
<td>Passive Protection</td>
<td>Active Protection</td>
</tr>
</tbody>
</table>

![Bar Chart](chart.png)
Results ROV Enforcement

ROV enforcement differs by AS type
Results ROV Enforcement

IXP ROV is a special case
IXP Routeservers

Routeservers can only protect connected systems with ROV
Low Enforcement in IXPs?

Many paths over direct peerings
Impact of ROV on Spread of Hijacks
What is the Impact of ROV?

Internet graph observed with Traceroute
What is the Impact of ROV?

Impact is visible in propagation graph
What is the Impact of ROV?

<table>
<thead>
<tr>
<th>Graph Parameters</th>
<th>$G_1$</th>
<th>$G_2$</th>
<th>$G_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertices</td>
<td>2156</td>
<td>2156</td>
<td>2156</td>
</tr>
<tr>
<td>Edges</td>
<td>3810</td>
<td>1974</td>
<td>3173</td>
</tr>
<tr>
<td>Components</td>
<td>1</td>
<td>808</td>
<td>35</td>
</tr>
<tr>
<td>Largest Component</td>
<td>2156</td>
<td>1315</td>
<td>2110</td>
</tr>
<tr>
<td>Avg. Node-Degree</td>
<td>1.77</td>
<td>0.90</td>
<td>1.47</td>
</tr>
<tr>
<td>Avg. Algebraic-Connectivity</td>
<td>187.97</td>
<td>6.29</td>
<td>21.68</td>
</tr>
<tr>
<td>Avg. Shortest-Path Length</td>
<td>4.55</td>
<td>2.97</td>
<td>5.00</td>
</tr>
<tr>
<td>Avg. Longest-Path Length</td>
<td>9.52</td>
<td>5.78</td>
<td>9.34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>G1</th>
<th>G2</th>
<th>G3</th>
</tr>
</thead>
<tbody>
<tr>
<td>No ROV</td>
<td>All ROV</td>
<td>IXP ROV</td>
<td></td>
</tr>
</tbody>
</table>
### What is the Impact of ROV?

ROV reduces connectivity for hijacks

<table>
<thead>
<tr>
<th>Graph Parameters</th>
<th>$G_1$</th>
<th>$G_2$</th>
<th>$G_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertices</td>
<td>2156</td>
<td>2156</td>
<td>2156</td>
</tr>
<tr>
<td>Edges</td>
<td>3810</td>
<td>1974</td>
<td>3173</td>
</tr>
<tr>
<td>Components</td>
<td>1</td>
<td>808</td>
<td>35</td>
</tr>
<tr>
<td>Largest Component</td>
<td>2156</td>
<td>1315</td>
<td>2110</td>
</tr>
<tr>
<td>Avg. Node-Degree</td>
<td>1.77</td>
<td>0.90</td>
<td>1.47</td>
</tr>
<tr>
<td>Avg. Algebraic-Connectivity</td>
<td>187.97</td>
<td>6.29</td>
<td>21.68</td>
</tr>
<tr>
<td>Avg. Shortest-Path Length</td>
<td>4.55</td>
<td>2.97</td>
<td>5.00</td>
</tr>
<tr>
<td>Avg. Longest-Path Length</td>
<td>9.52</td>
<td>5.78</td>
<td>9.34</td>
</tr>
</tbody>
</table>
What is the Impact of ROV?

<table>
<thead>
<tr>
<th>Graph Parameters</th>
<th>$G_1$</th>
<th>$G_2$</th>
<th>$G_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertices</td>
<td>2156</td>
<td>2156</td>
<td>2156</td>
</tr>
<tr>
<td>Edges</td>
<td>3810</td>
<td>1974</td>
<td>3173</td>
</tr>
<tr>
<td>Components</td>
<td>1</td>
<td>808</td>
<td>35</td>
</tr>
<tr>
<td>Largest Component</td>
<td>2156</td>
<td>1315</td>
<td>2110</td>
</tr>
<tr>
<td>Avg. Node-Degree</td>
<td>1.77</td>
<td>0.90</td>
<td>1.47</td>
</tr>
<tr>
<td>Avg. Algebraic-Connectivity</td>
<td>187.97</td>
<td>6.29</td>
<td>21.68</td>
</tr>
<tr>
<td>Avg. Shortest-Path Length</td>
<td>4.55</td>
<td>2.97</td>
<td>5.00</td>
</tr>
<tr>
<td>Avg. Longest-Path Length</td>
<td>9.52</td>
<td>5.78</td>
<td>9.34</td>
</tr>
</tbody>
</table>

IXP ROV barely prevents global spread of hijacks
Takeaways
Takeaways

- Enforcing ROV protects your own and other systems
- When no ROV is deployed, moving sessions to the routeserver minimizes the attack surface
- Even without ROV, you can benefit from the RPKI by creating ROAs
Thank you for your attention!

If you have any other questions, contact me at niklas.vogel@sit.fraunhofer.de

This talk is based on our publication: https://arxiv.org/abs/2303.11772