ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

SAN DIEGO
N89
2023

The complex reality of protecting BGP

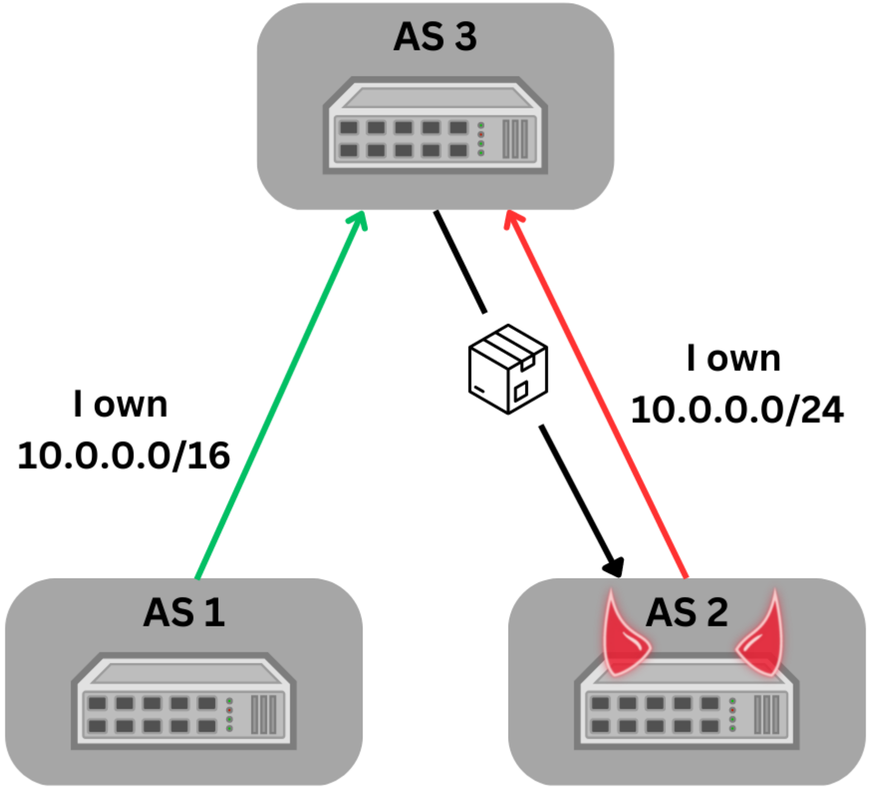
Quantifying the impact of RPKI validation in ISPs and IXPs

Niklas Vogel, and Haya Shulman

German National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT
Goethe University Frankfurt

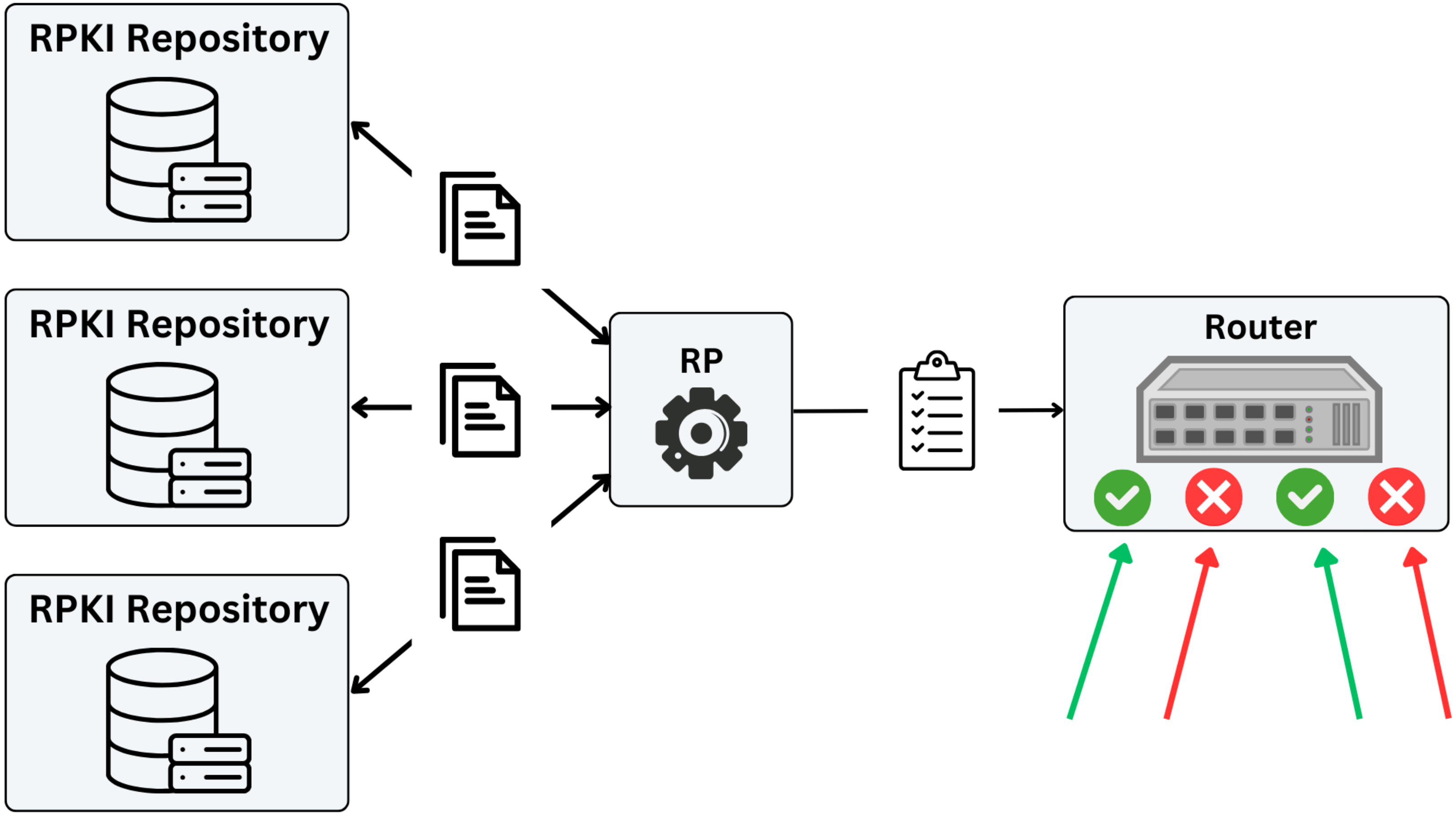
Motivation BGP and RPKI

The inherent Hijack-Problem in BGP



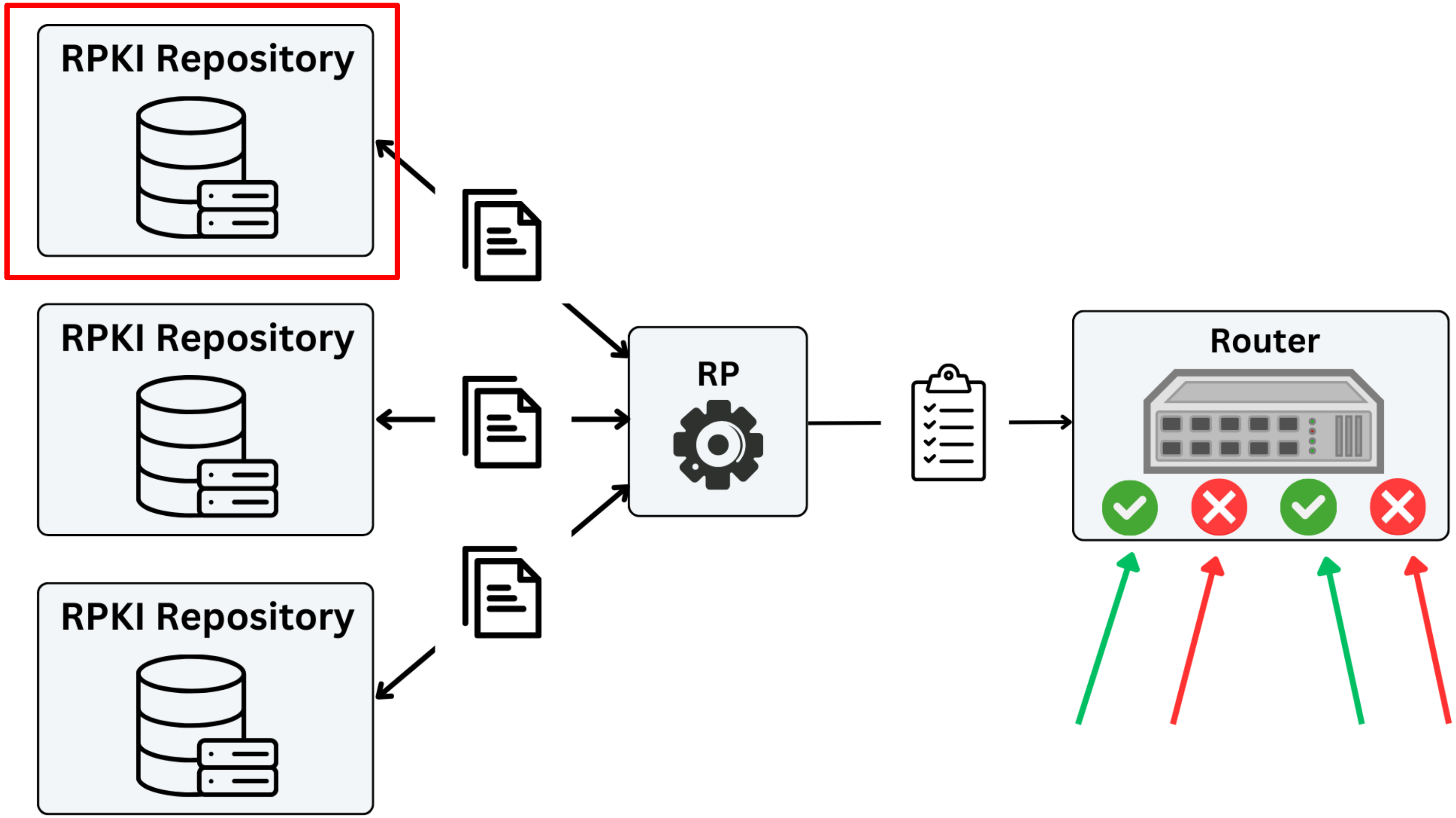
Attackers can hijack IP traffic

Preventing Hijacks with the RPKI



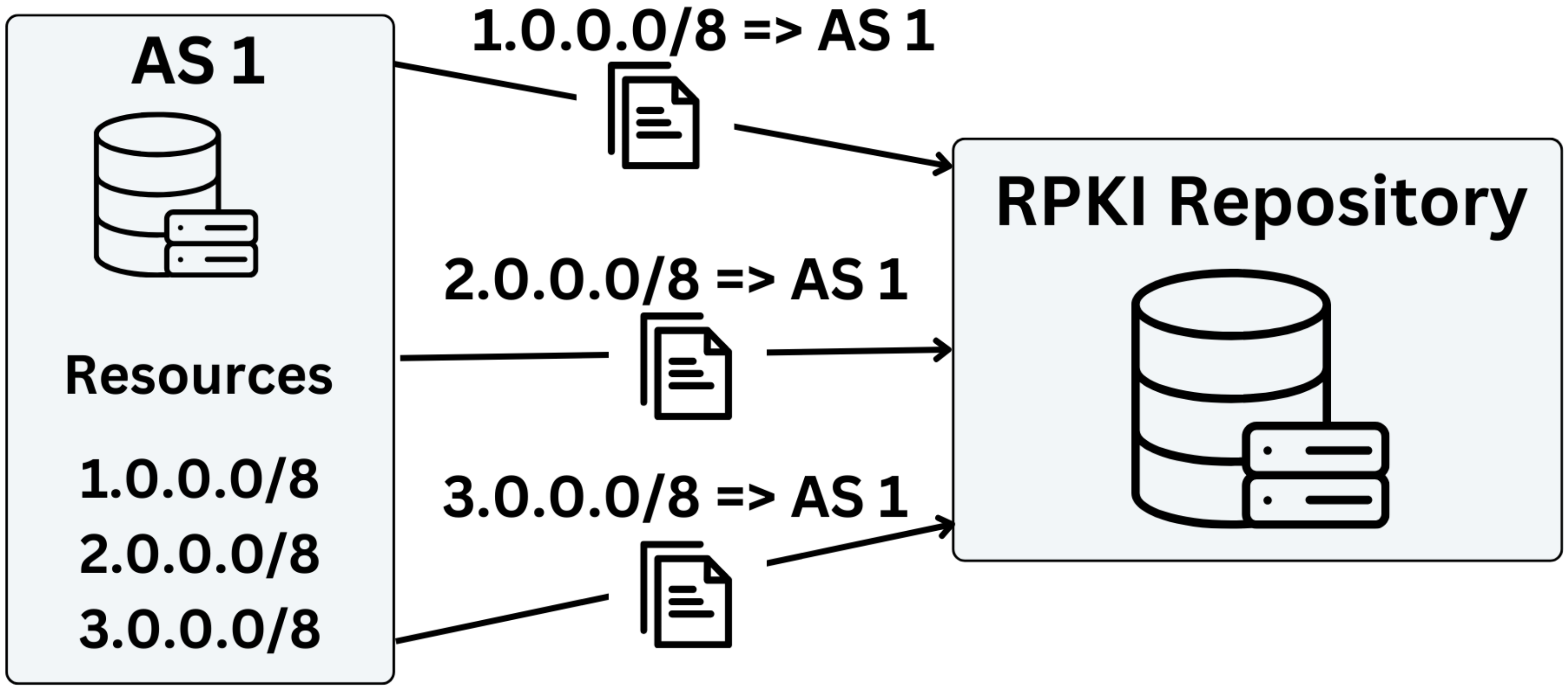
RPKI prevents Hijacks

Preventing Hijacks with the RPKI



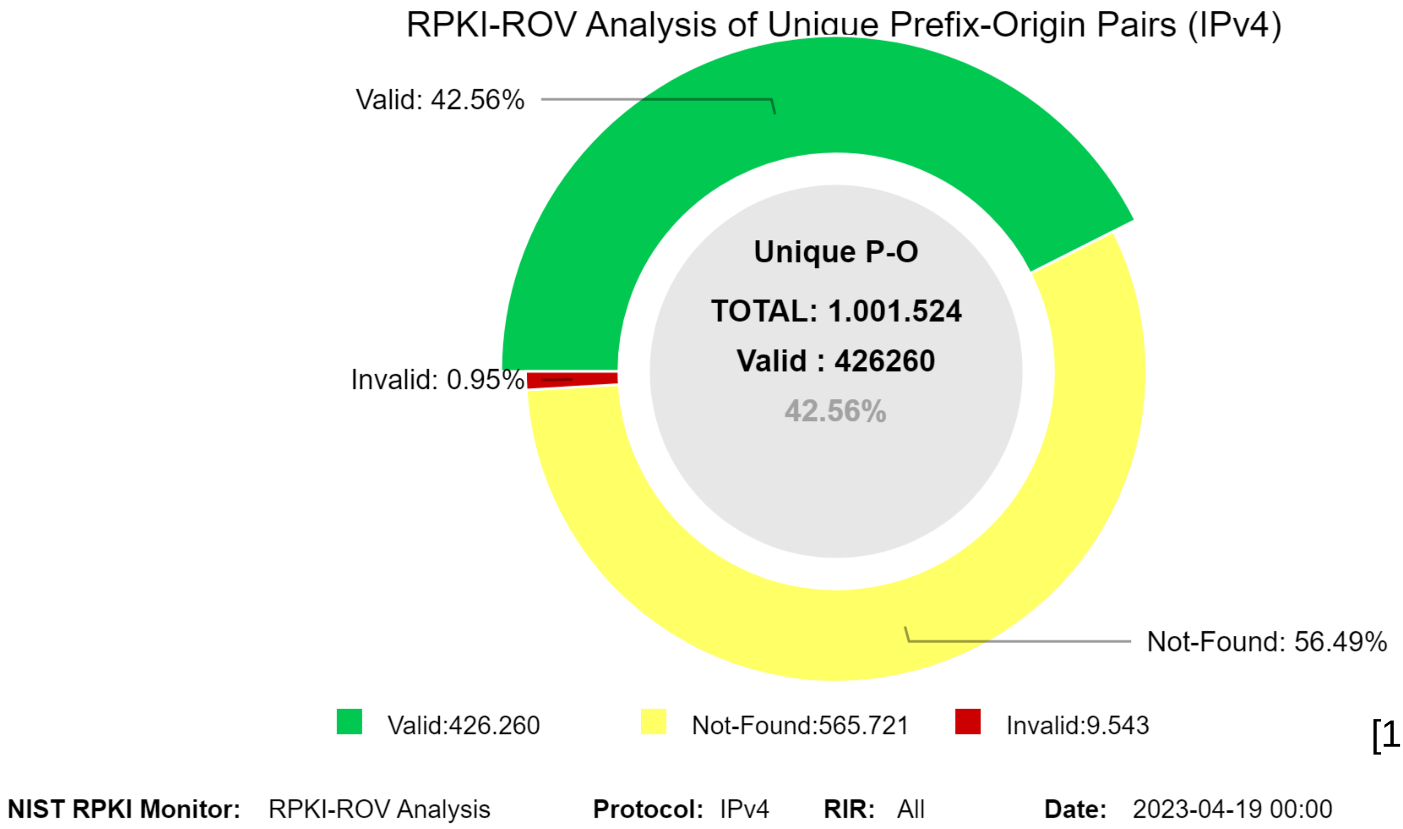
Publication Section

Preventing Hijacks with the RPKI



Systems publish ROAS

How many Systems publish ROAs?



RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)

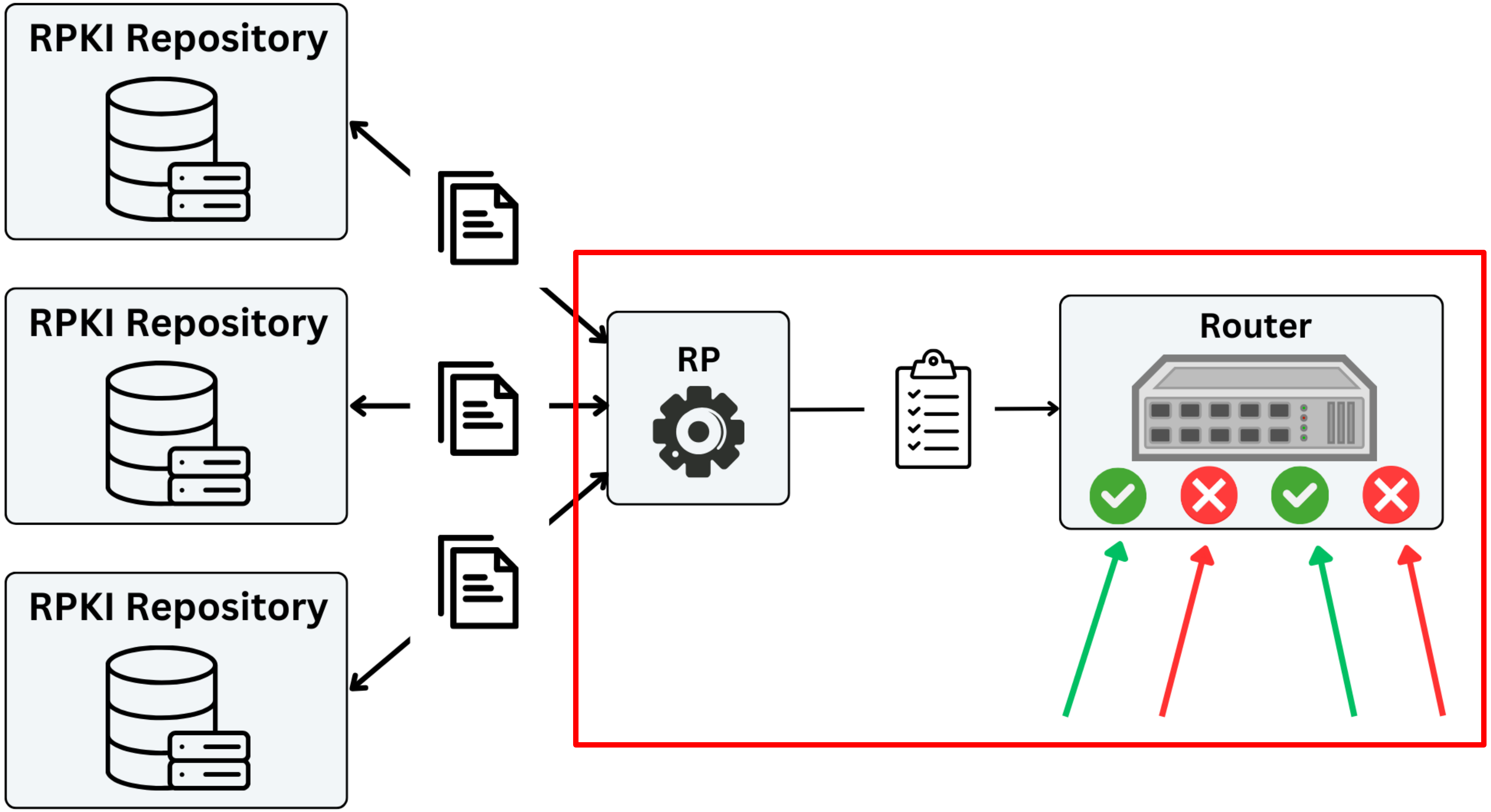
NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All **Date:** 2023-04-19 00:00

[1]

<u>Adaption of RPKI is increasing</u>

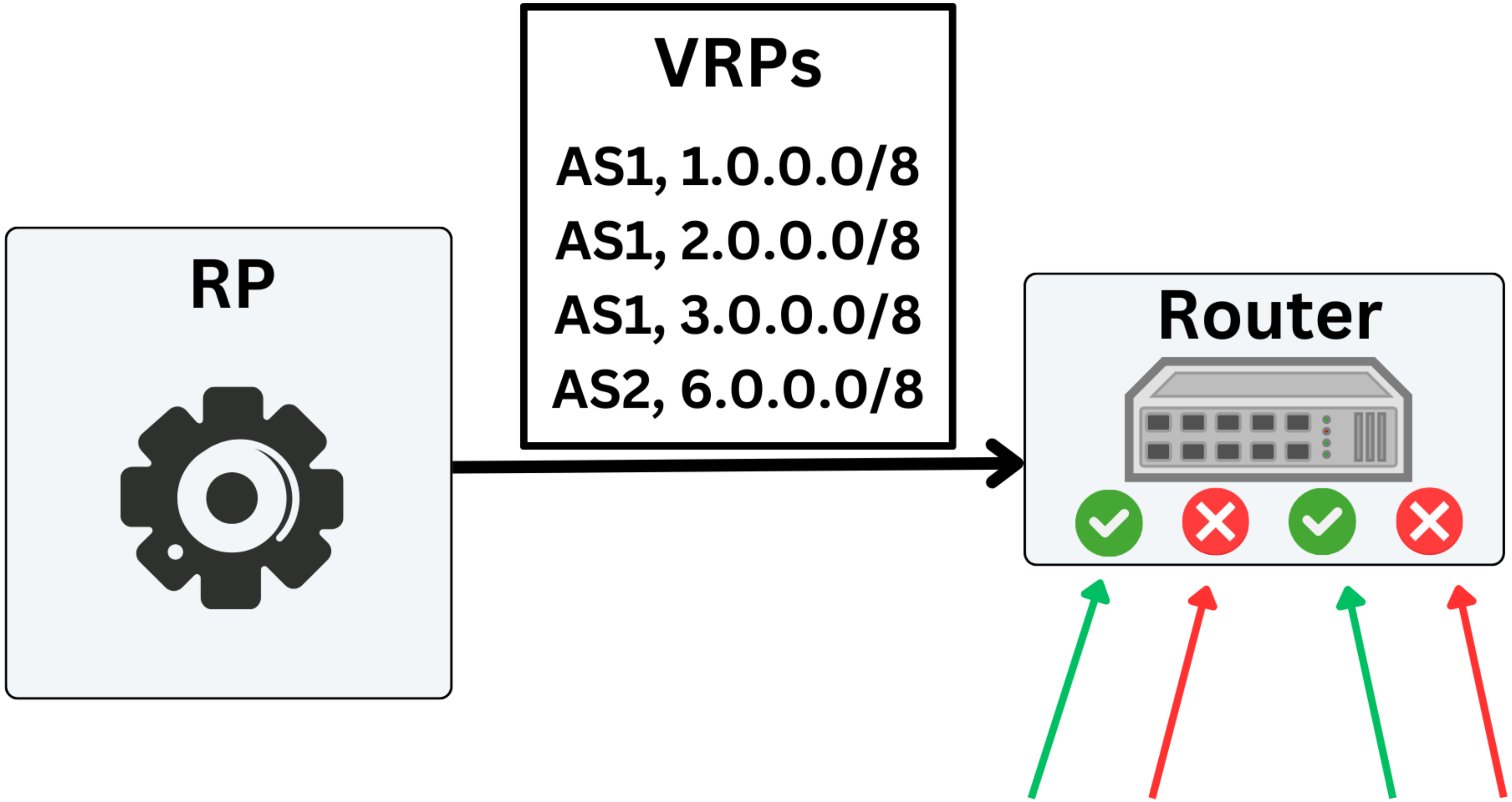
[1]: https://rpki-monitor.antd.nist.gov/ (Accessed 19.04.2023)

Preventing Hijacks with the RPKI



Enforcement Section

Preventing Hijacks with the RPKI



Routers enforce ROV

How many Systems enforce ROV?

Project Name	Year	ROV
Cloudflare [1]	2023	30%
APNIC [2]	2023	29.3%
Rodday et al. [3]	2021	0.6%

30% of Systems enforce ROV

[1]: https://isbgpsafeyet.com/ (Accessed 04.10.2023)
[2]: https://stats.labs.apnic.net/rpki (Accessed 04.10.2023)
[3]: https://par.nsf.gov/servlets/purl/10317492 (Accessed 04.10.2023)

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?

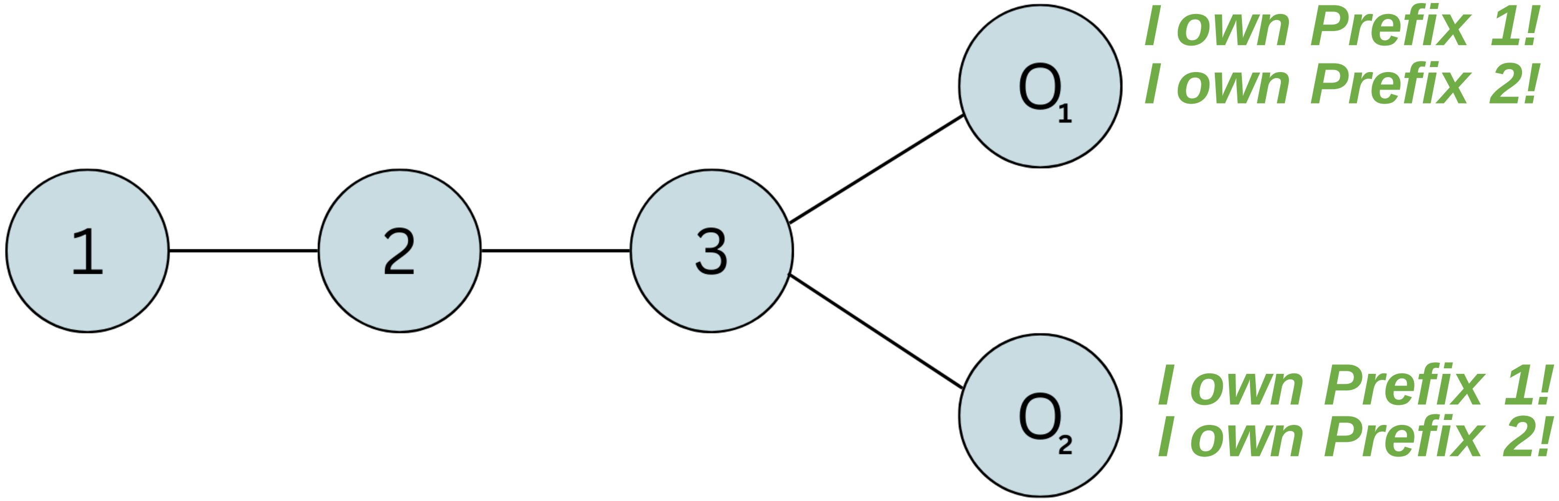
- **How to identify if a system enforces ROV?**
  - **=> Announce hijacks**

- **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?

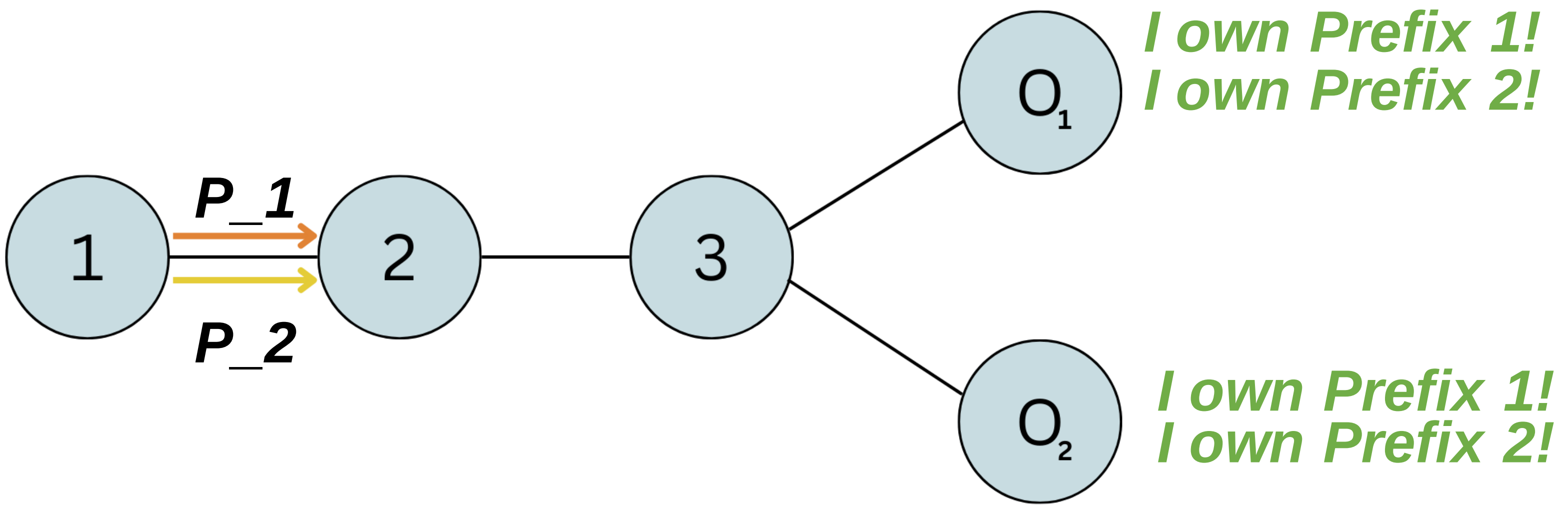
- **Setup: No RPKI**



Both prefixes are announced by both ASes

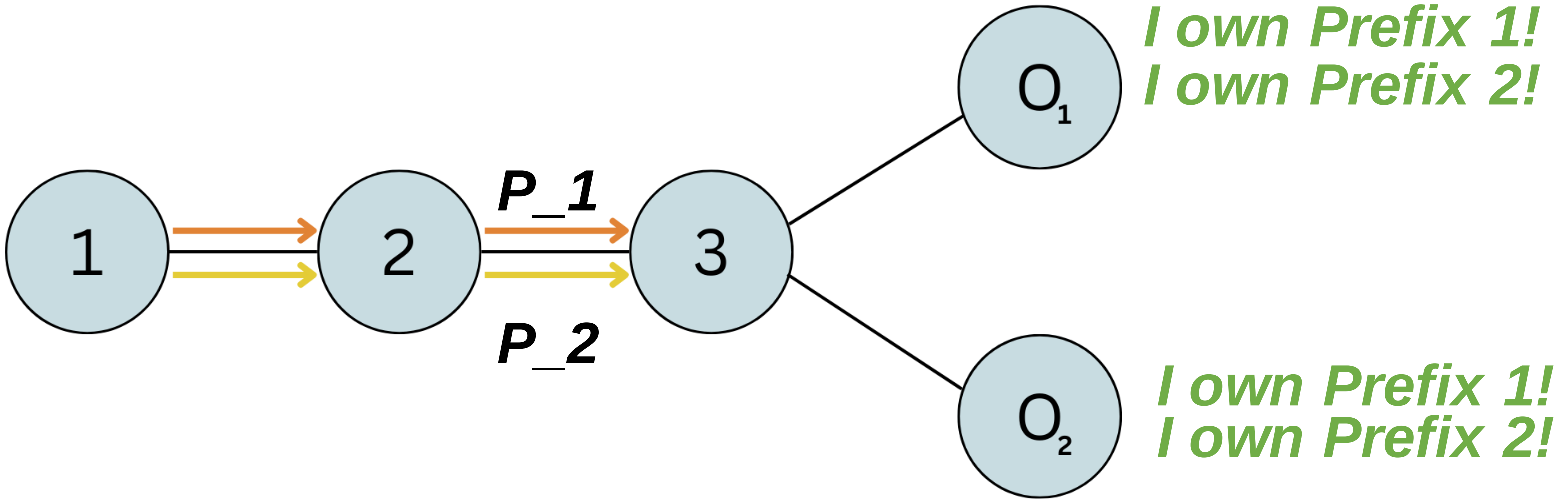
How to measure ROV Deployment?

- **Setup: No RPKI**



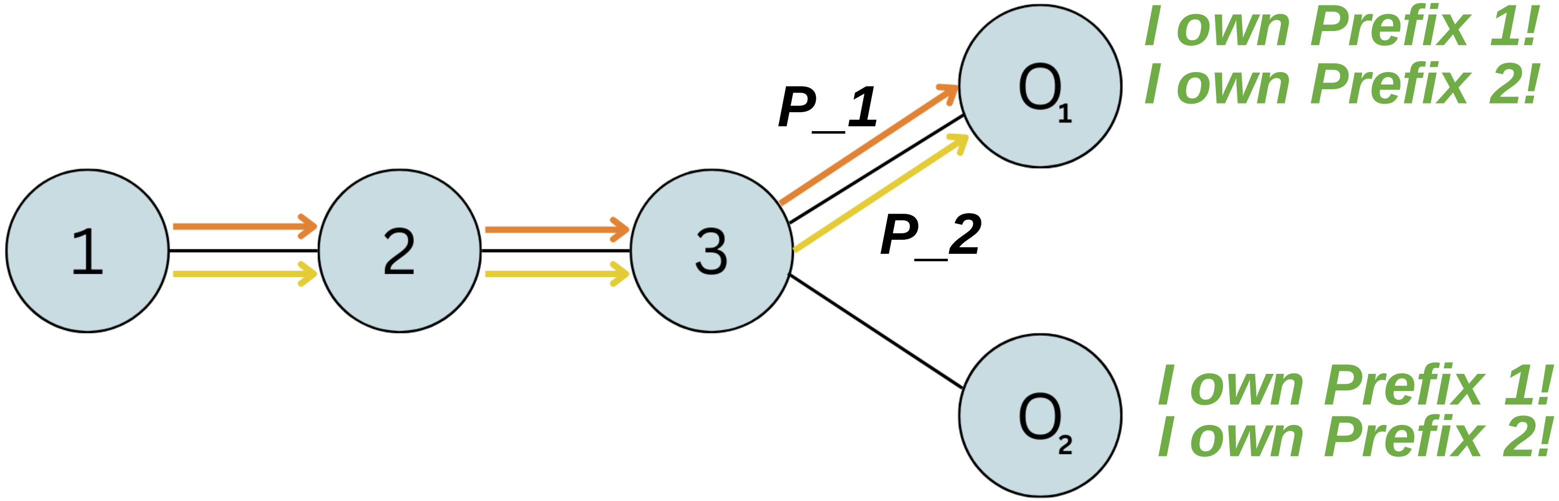
How to measure ROV Deployment?

- **Setup: No RPKI**



How to measure ROV Deployment?

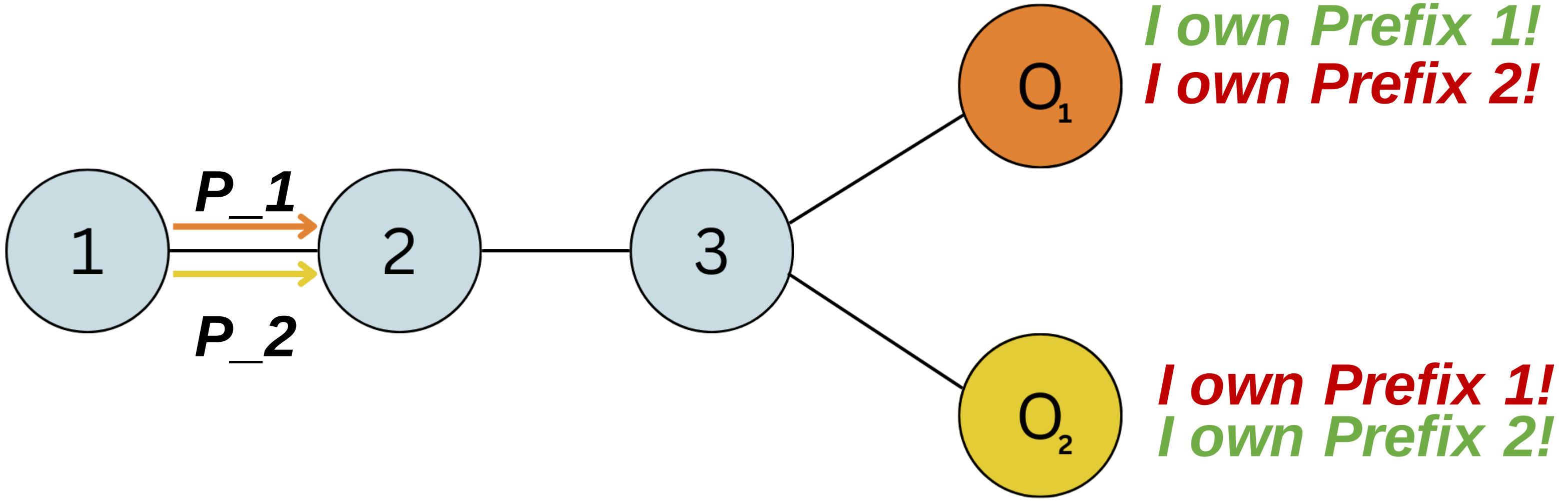
- **Setup: No RPKI**



<u>Prefixes routed identically</u>

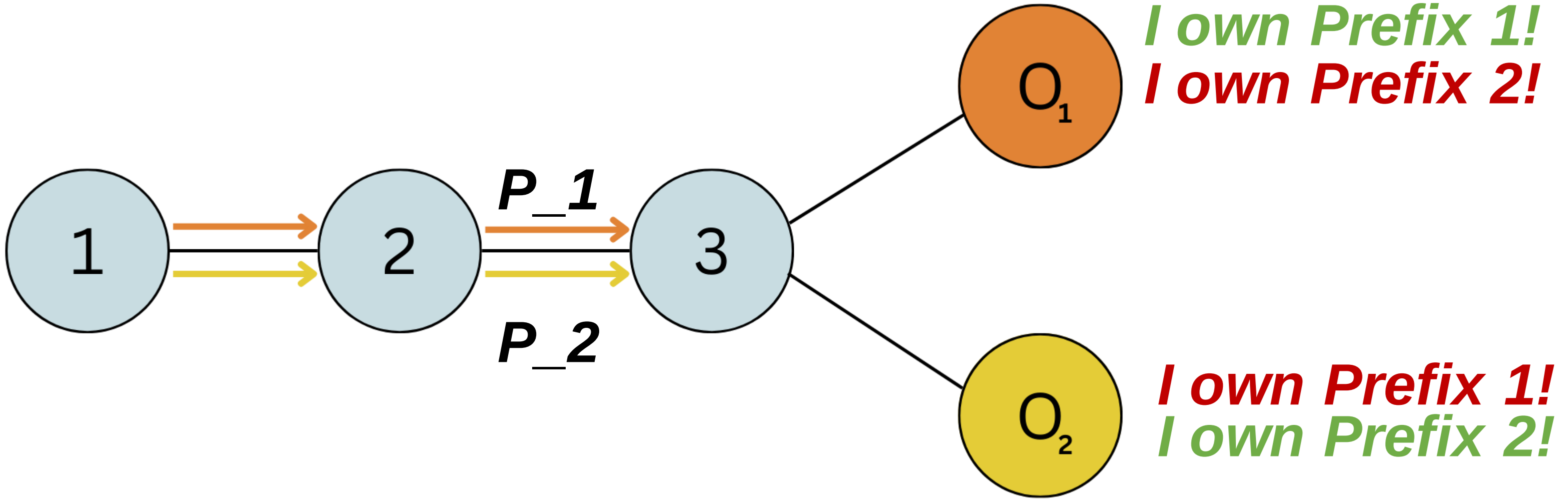
How to measure ROV Deployment?

- **With RPKI**



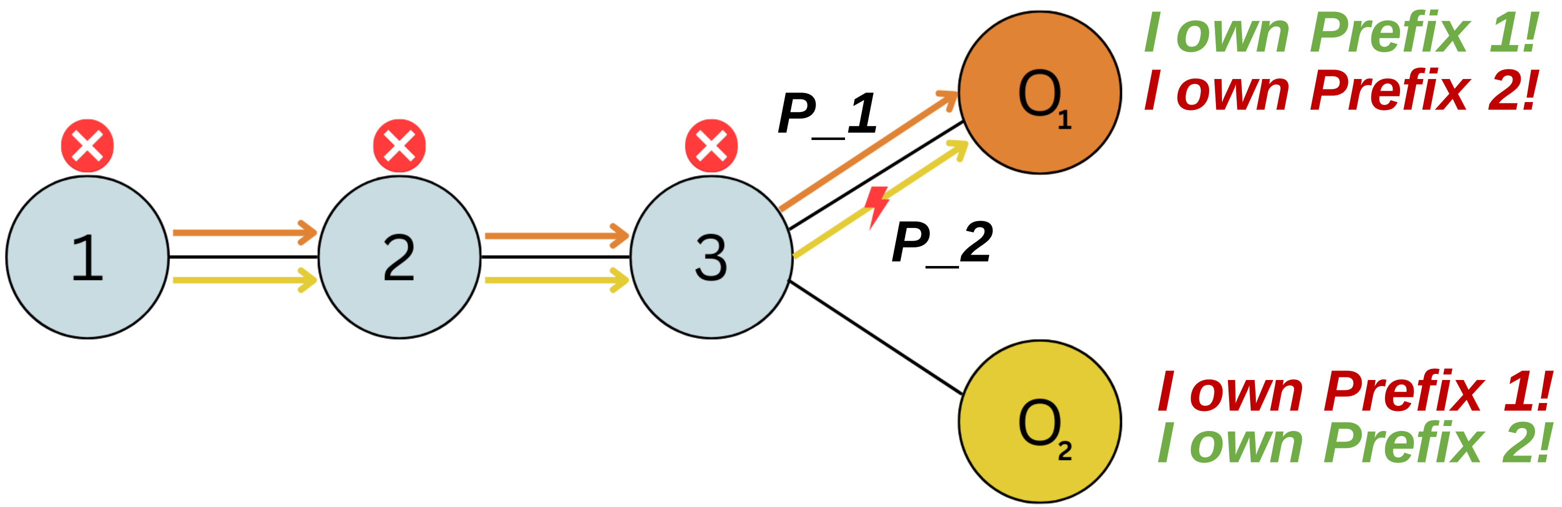
How to measure ROV Deployment?

- **With RPKI**



How to measure ROV Deployment?

- **With RPKI**

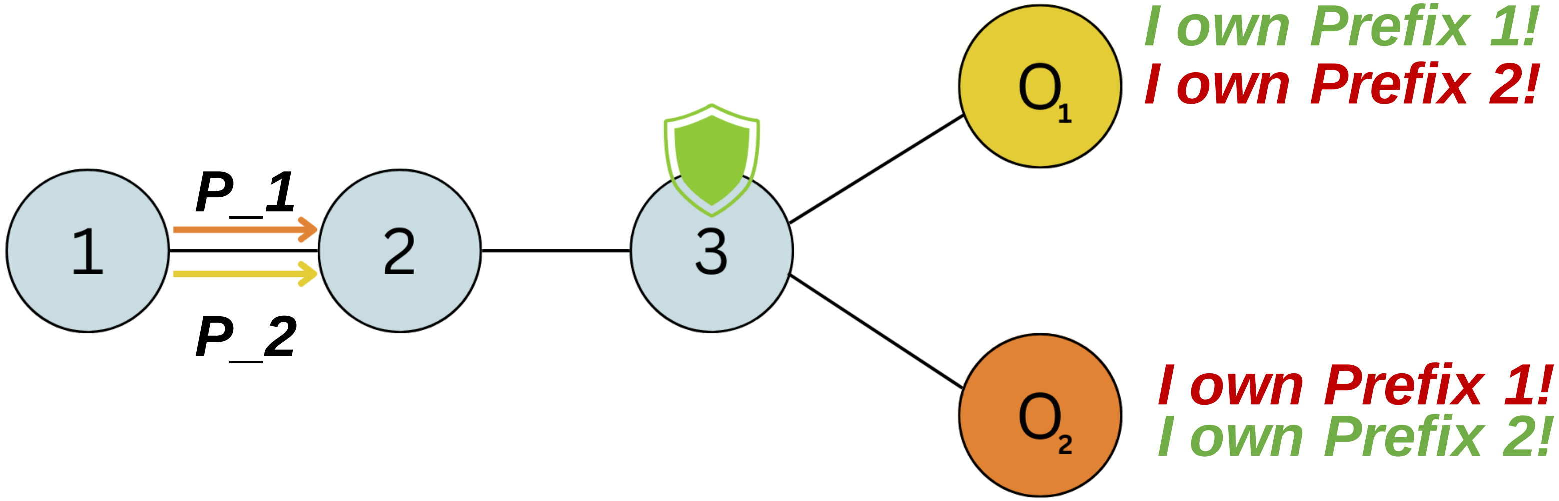


<u>Prefixes routed identically</u>

<u>No ROV in 1, 2, 3</u>

How to measure ROV Deployment?

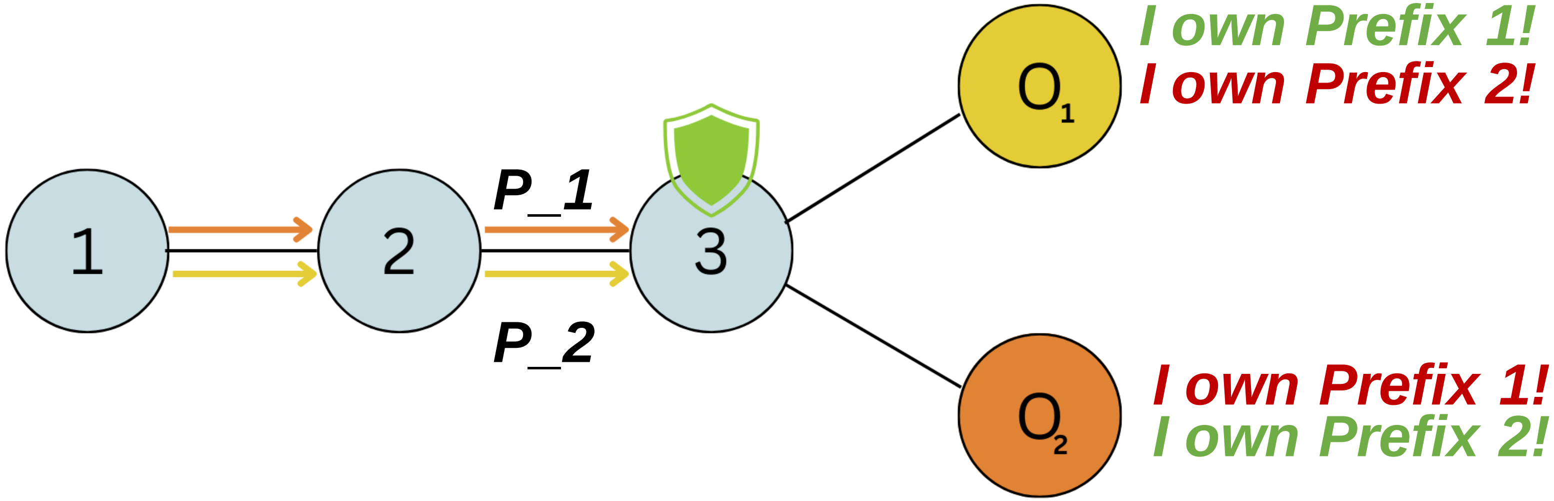
- **With ROV**



AS3 enforces ROV

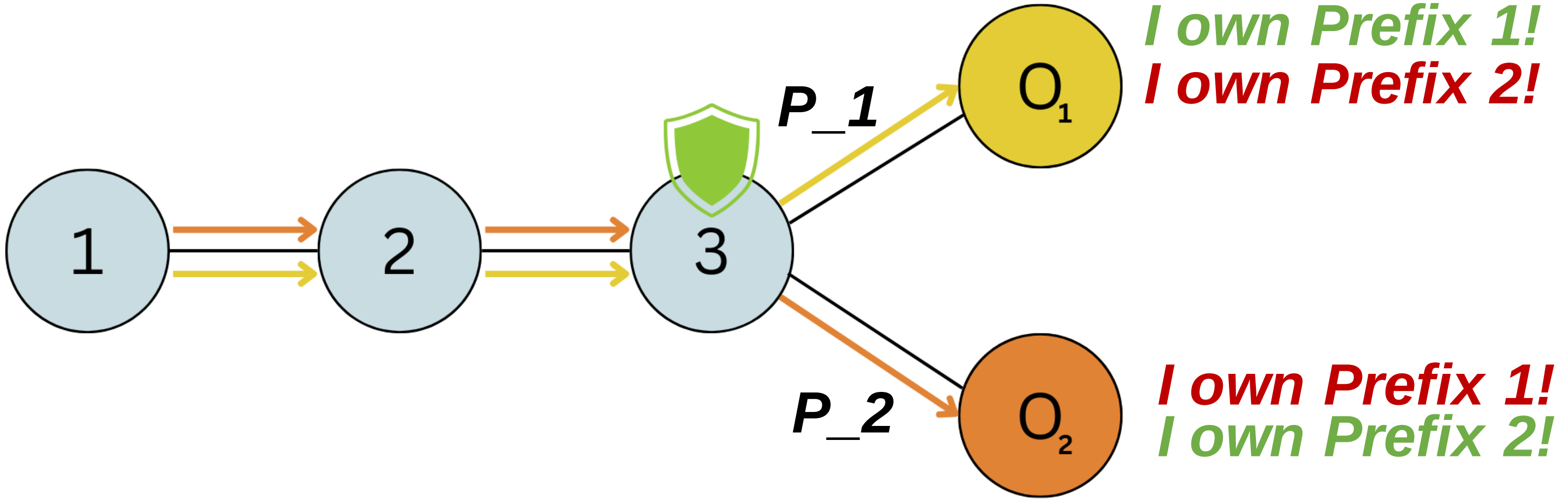
How to measure ROV Deployment?

- **With ROV**



How to measure ROV Deployment?

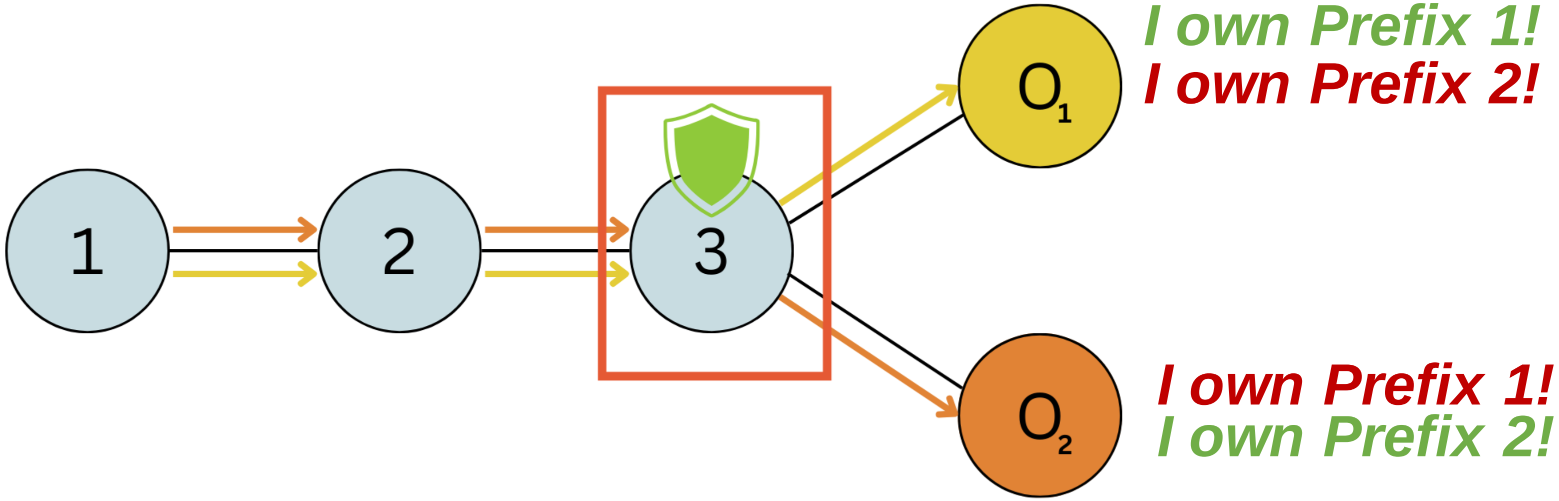
- **With ROV**



Prefix routing diverges

How to measure ROV Deployment?

- **With ROV**



Divergence Point enforces ROV

How to classify ROV Deployments?

- **No strict Enforcement**

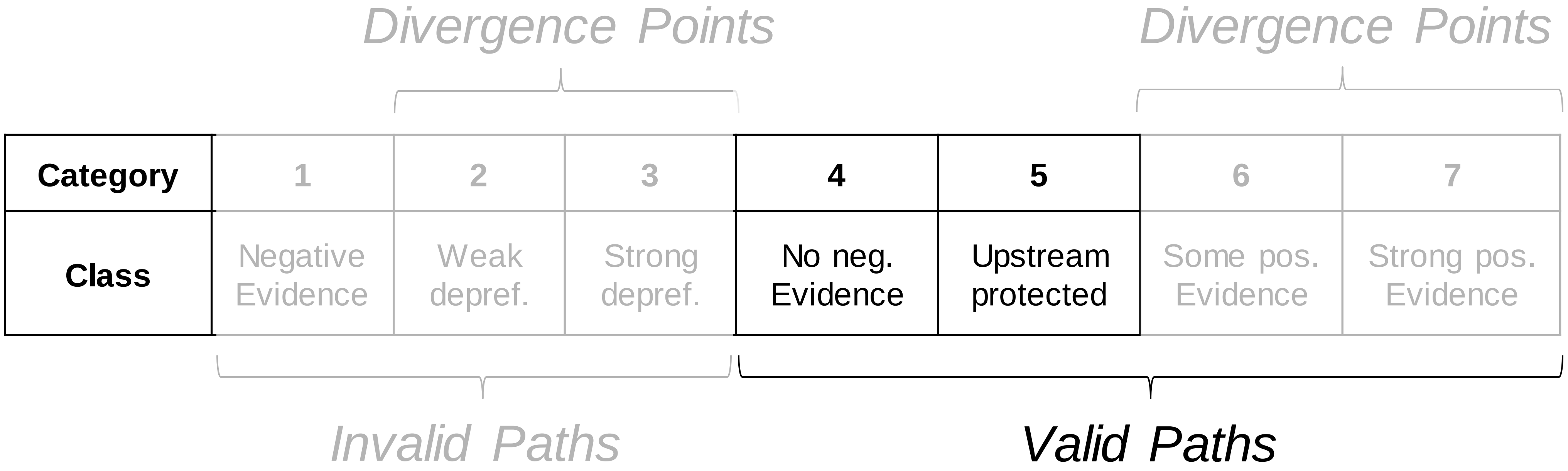
Divergence Points *Divergence Points*

Category	1	2	3	4	5	6	7
Class	Negative Evidence	Weak depref.	Strong depref.	No neg. Evidence	Upstream protected	Some pos. Evidence	Strong pos. Evidence

Invalid Paths *Valid Paths*

How to classify ROV Deployments?

- **Passive Protection**



Divergence Points

Divergence Points

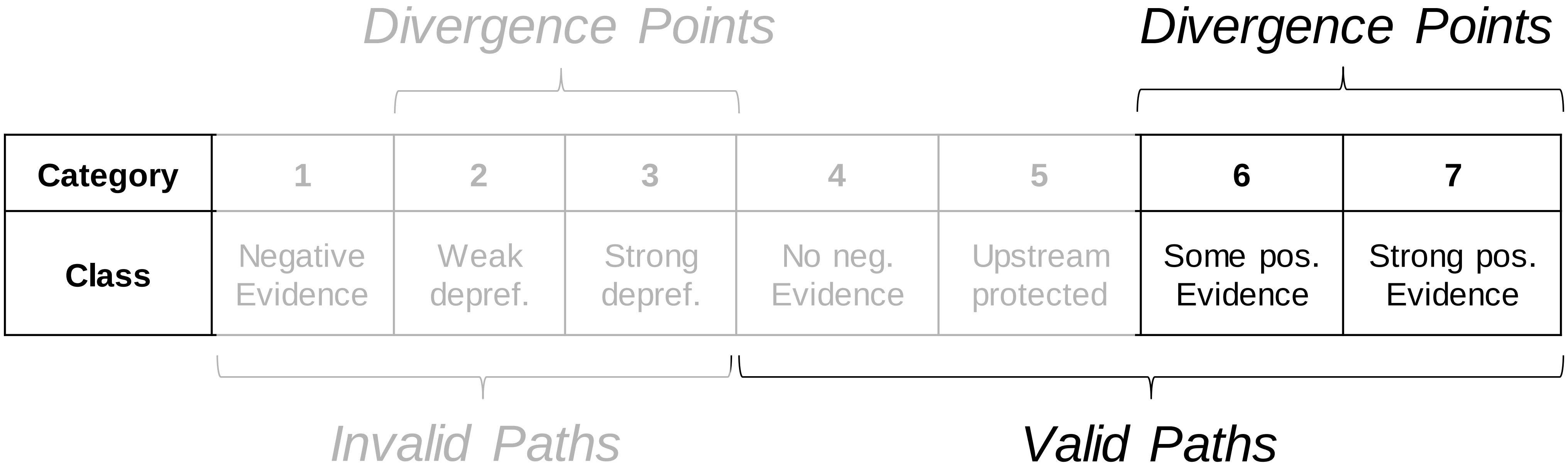
Category	1	2	3	4	5	6	7
Class	Negative Evidence	Weak depref.	Strong depref.	No neg. Evidence	Upstream protected	Some pos. Evidence	Strong pos. Evidence

Invalid Paths

Valid Paths

How to classify ROV Deployments?

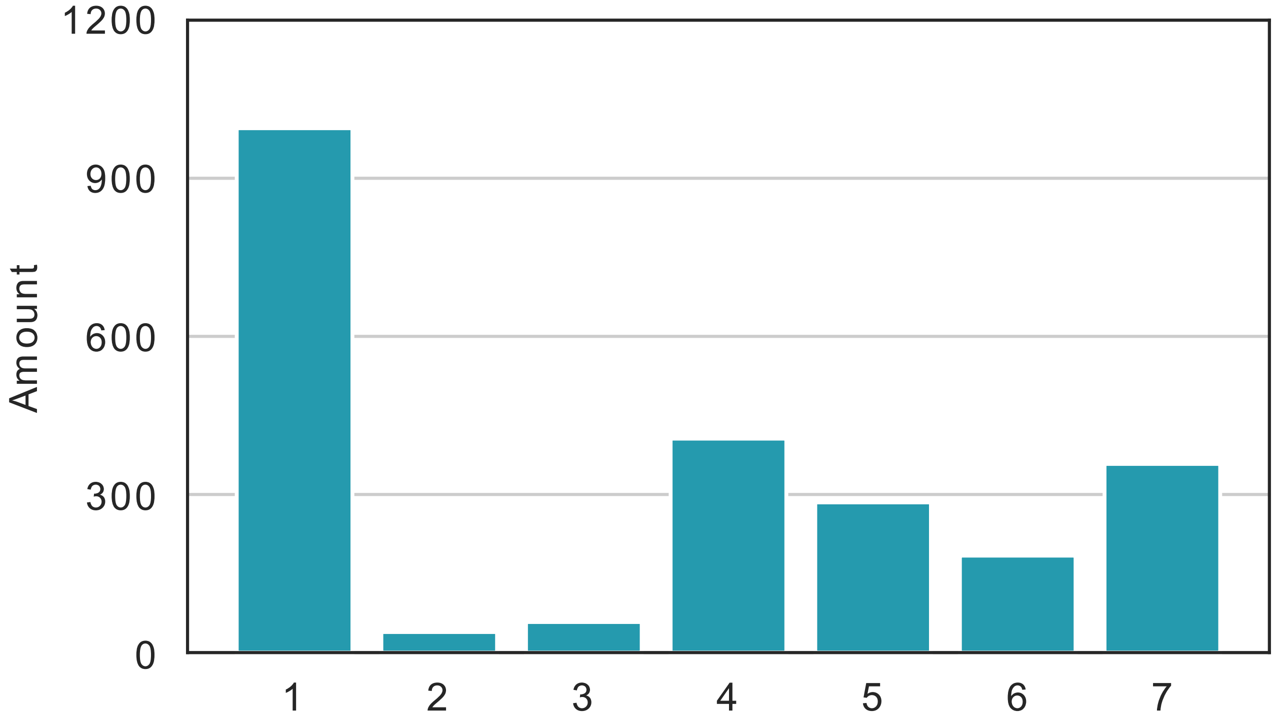
- **Active Protection**



Category	1	2	3	4	5	**6**	**7**
Class	Negative Evidence	Weak depref.	Strong depref.	No neg. Evidence	Upstream protected	Some pos. Evidence	Strong pos. Evidence

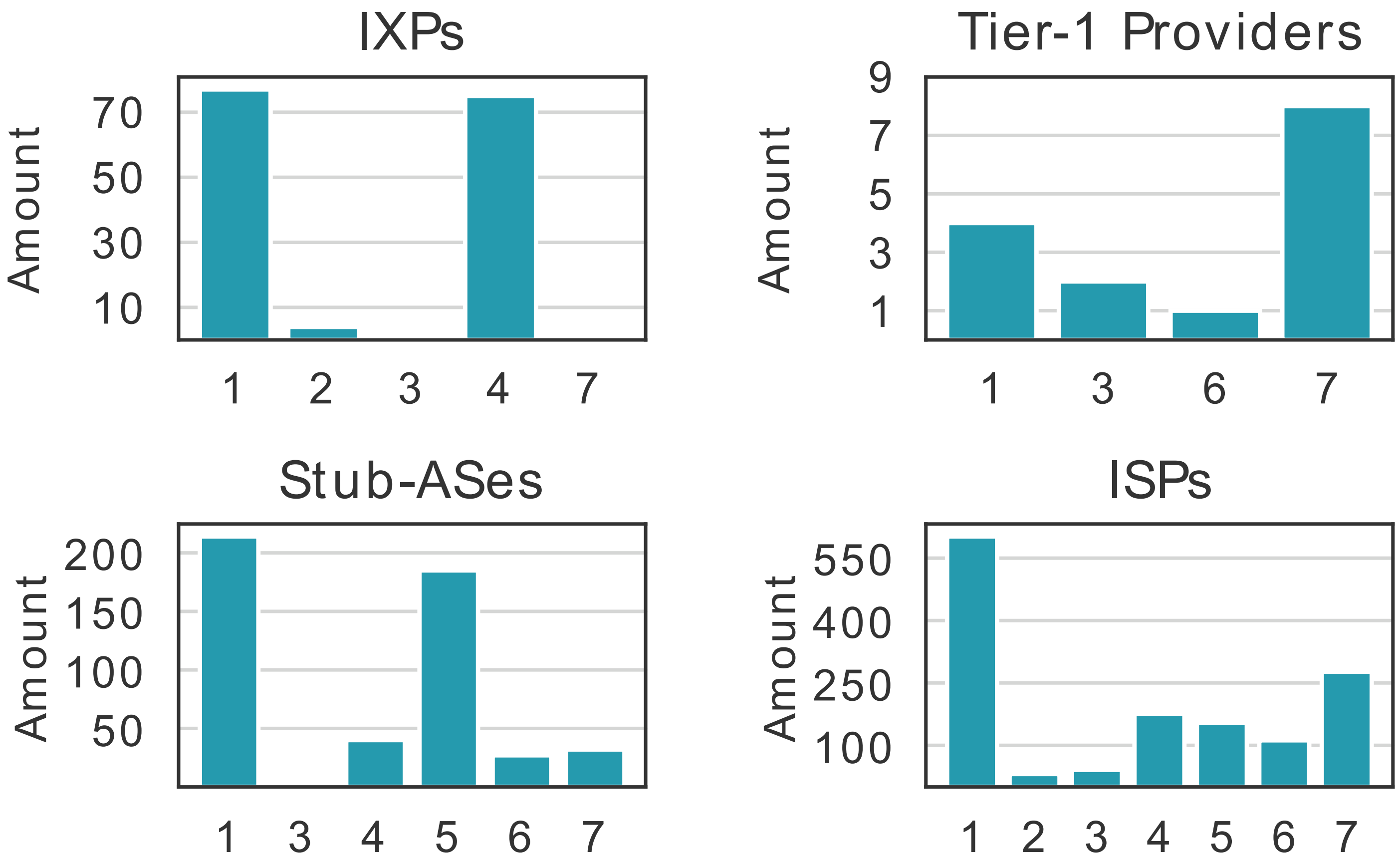
Measurement Results

Results ROV Enforcement



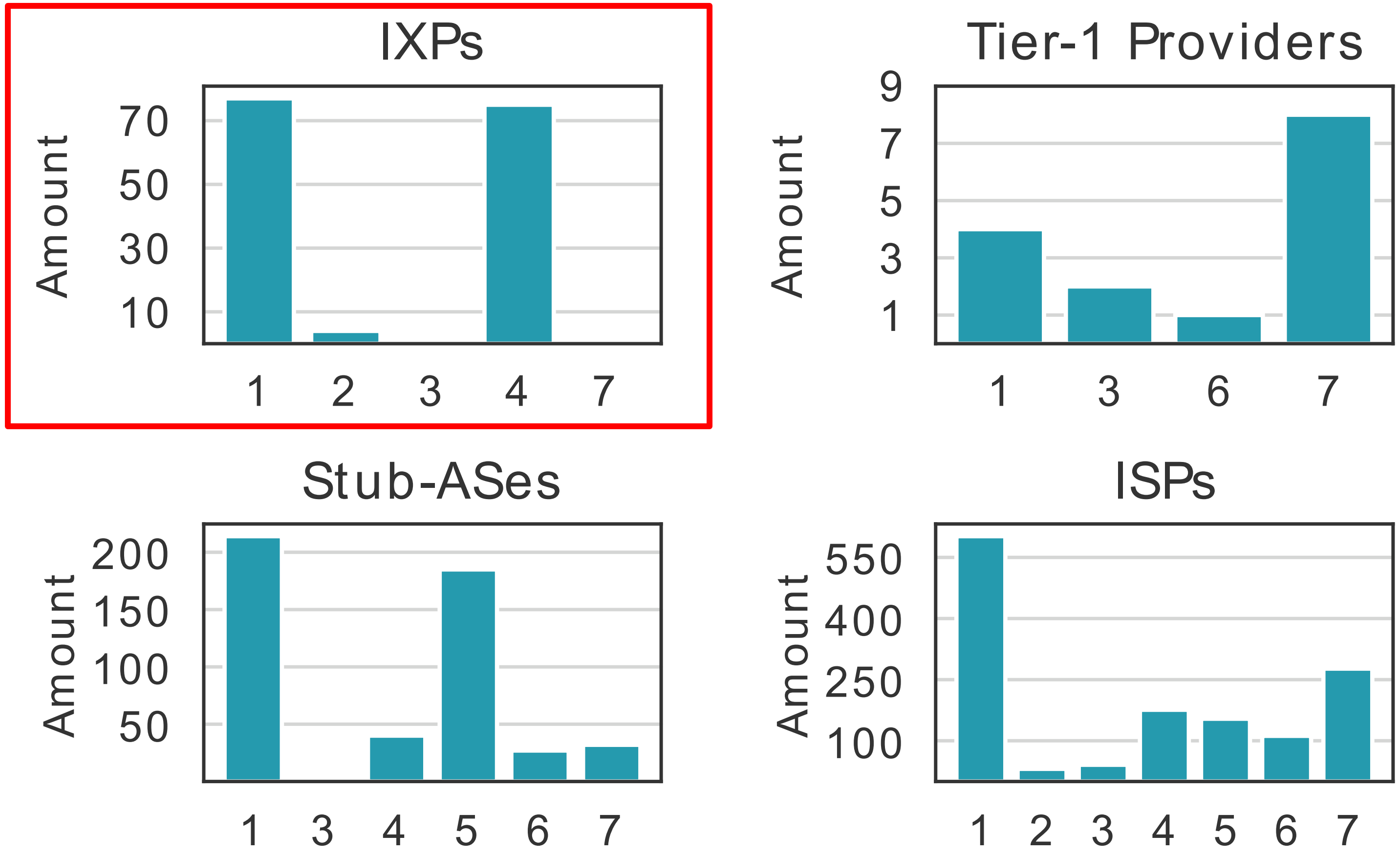
Category	1 - 3	4 - 5	6 - 7
Class	No strict Enforcement	Passive Protection	Active Protection

Results ROV Enforcement



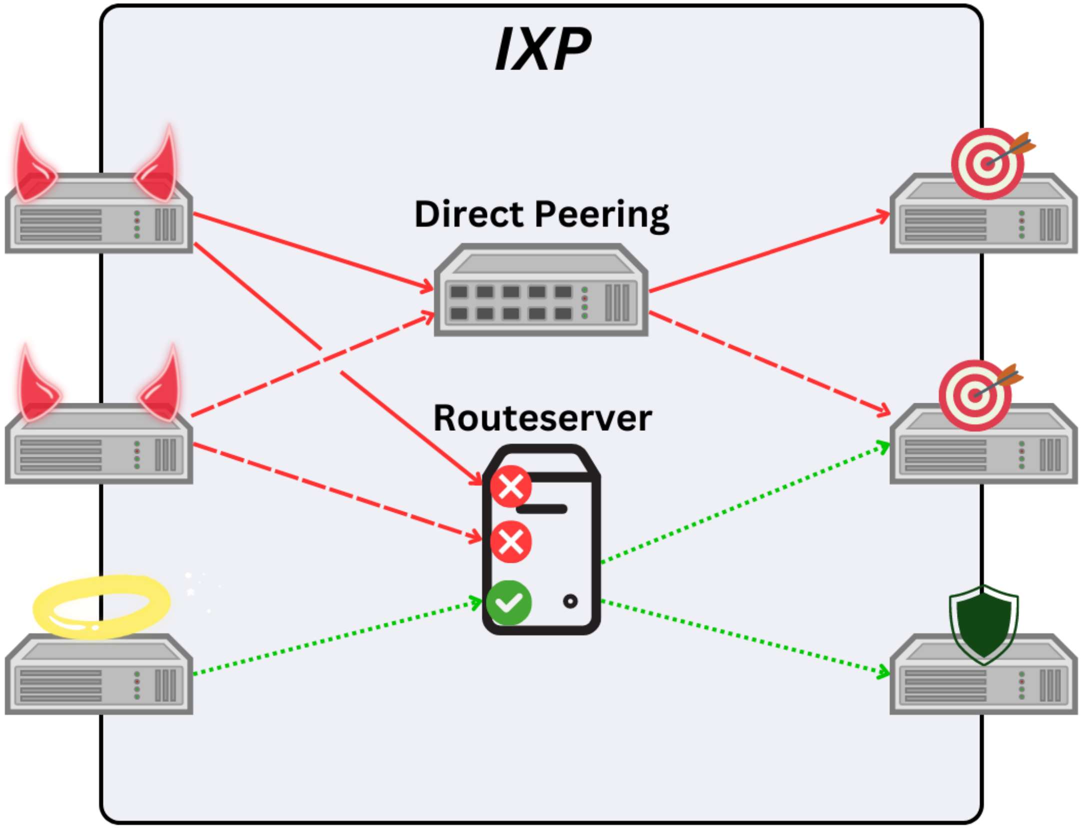
ROV enforcement differs by AS type

Results ROV Enforcement



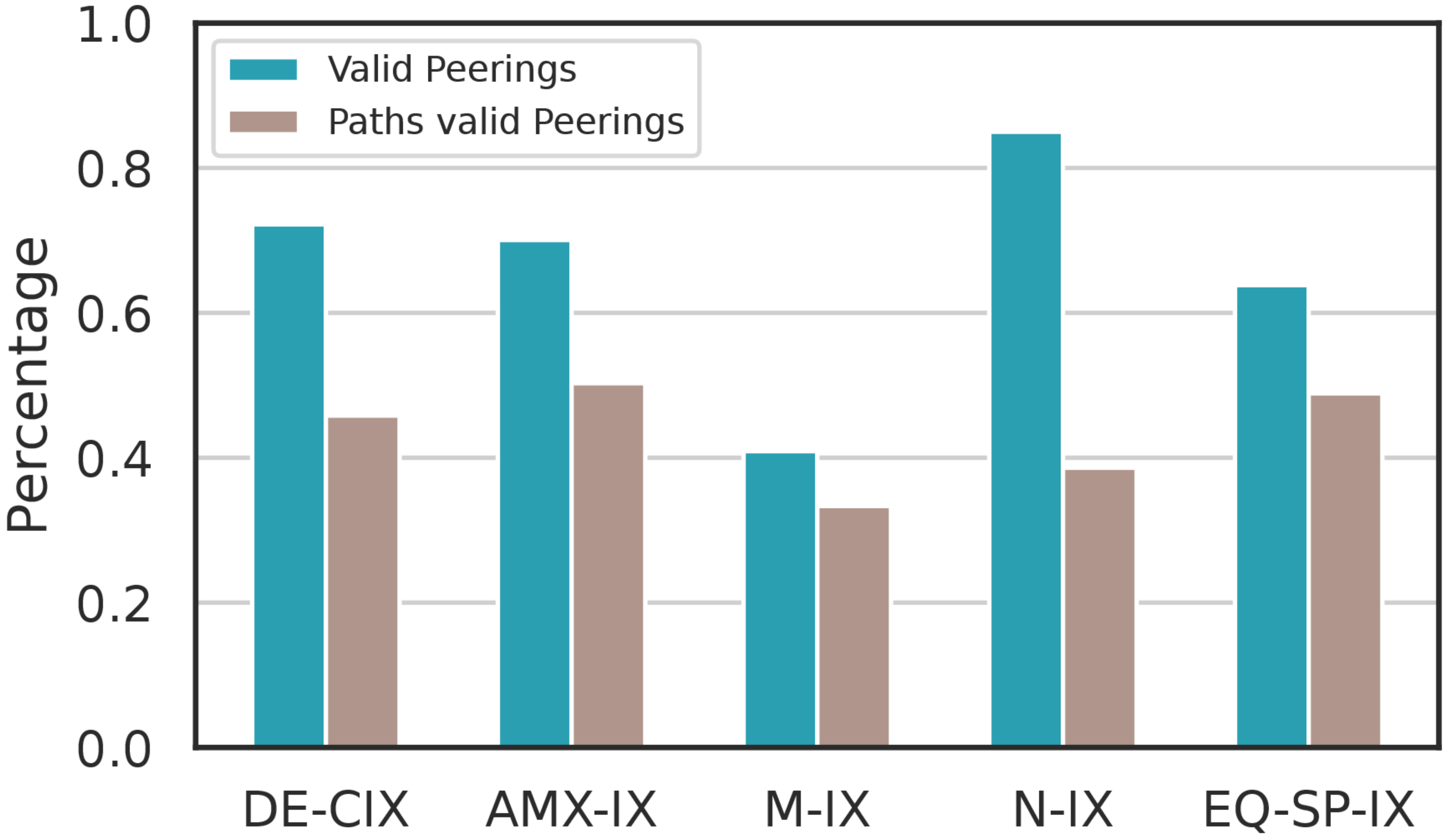
IXP ROV is a special case

IXP Routeservers



<u>Routeservers can only protect connected systems with ROV</u>

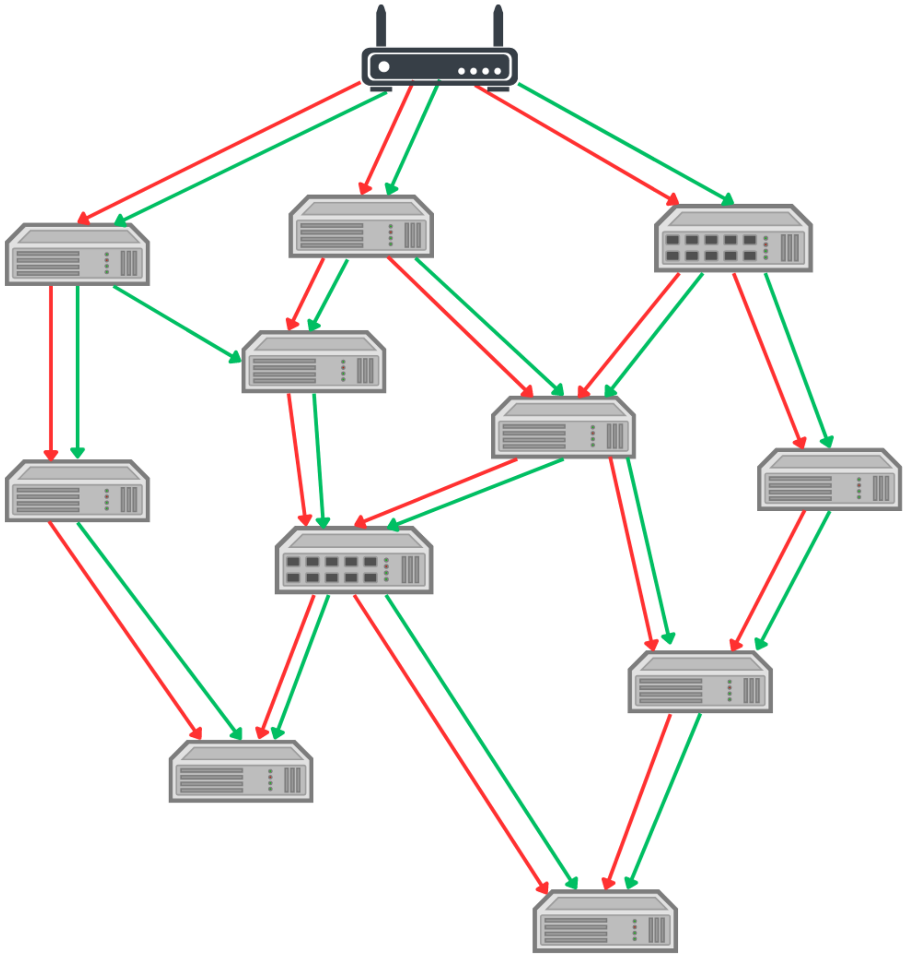
Low Enforcement in IXPs?



Many paths over direct peerings

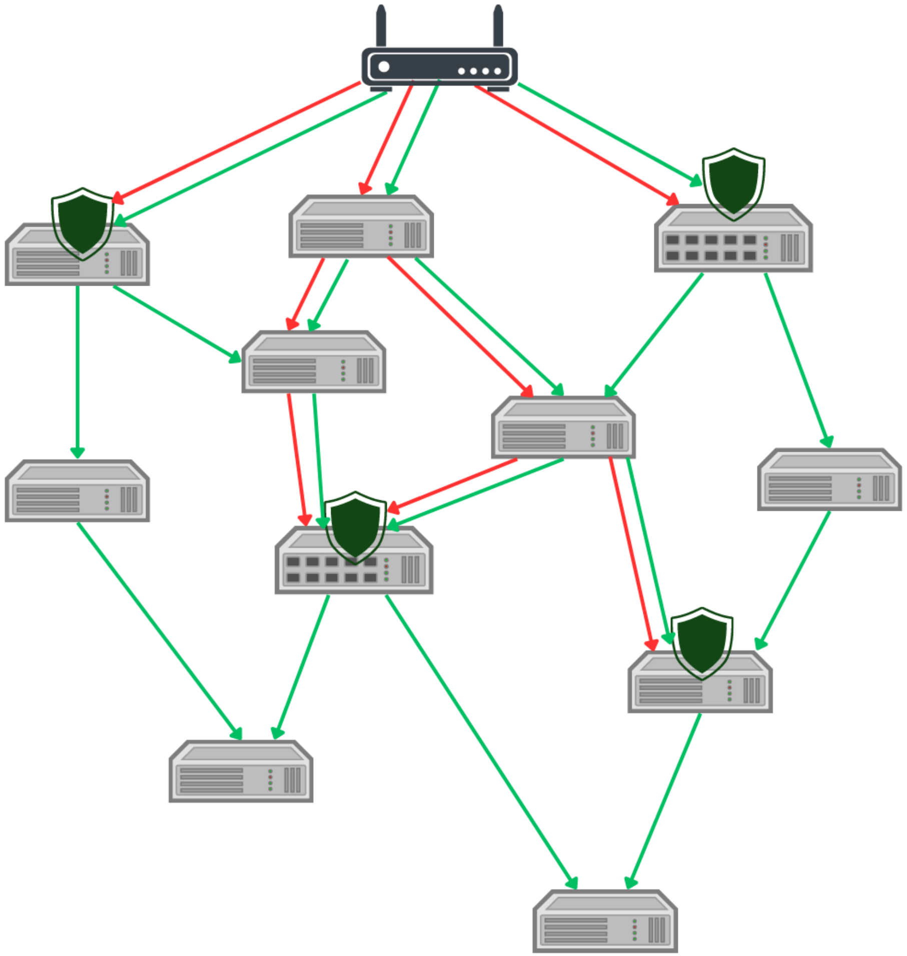
Impact of ROV on Spread of Hijacks

What is the Impact of ROV?



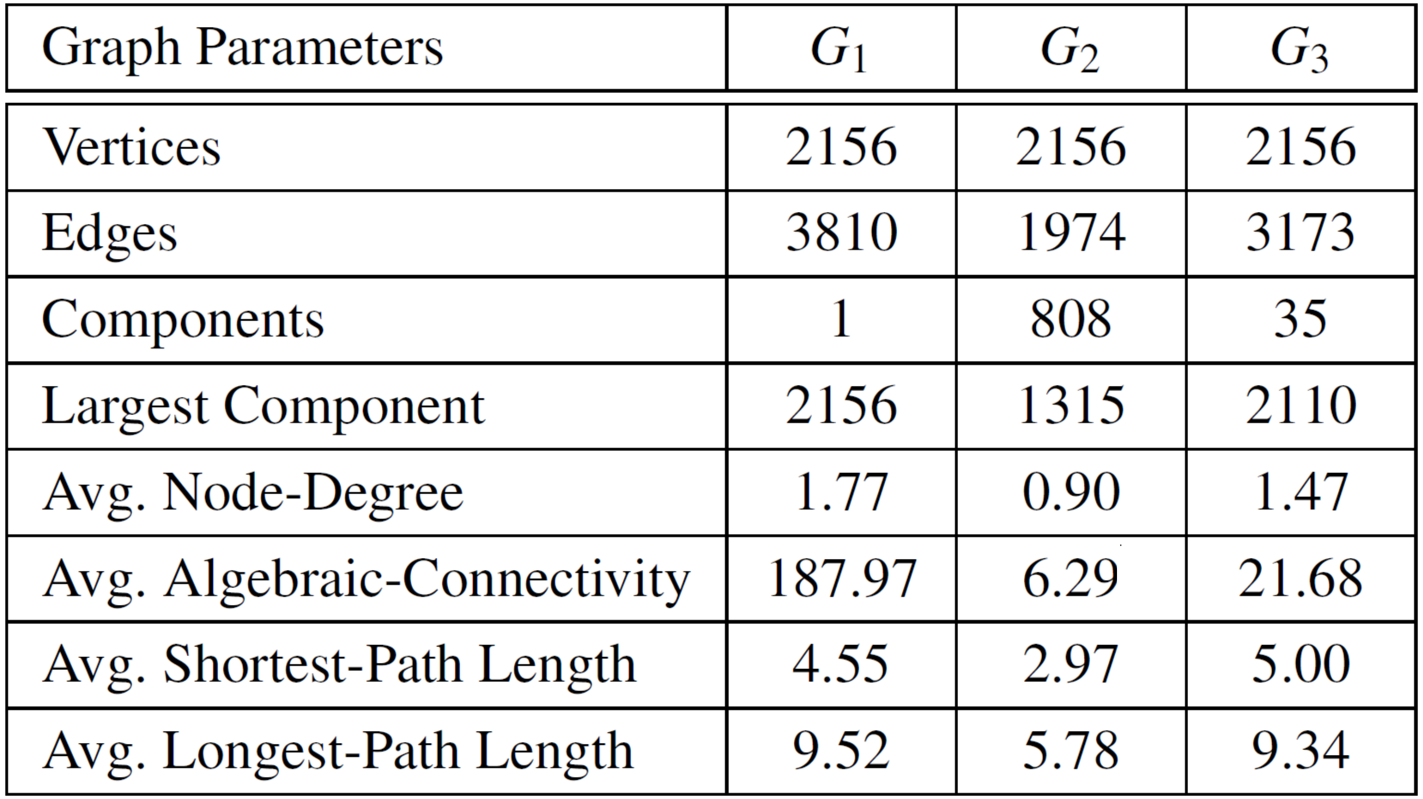
Internet graph observed with Traceroute

What is the Impact of ROV?



Impact is visible in propagation graph

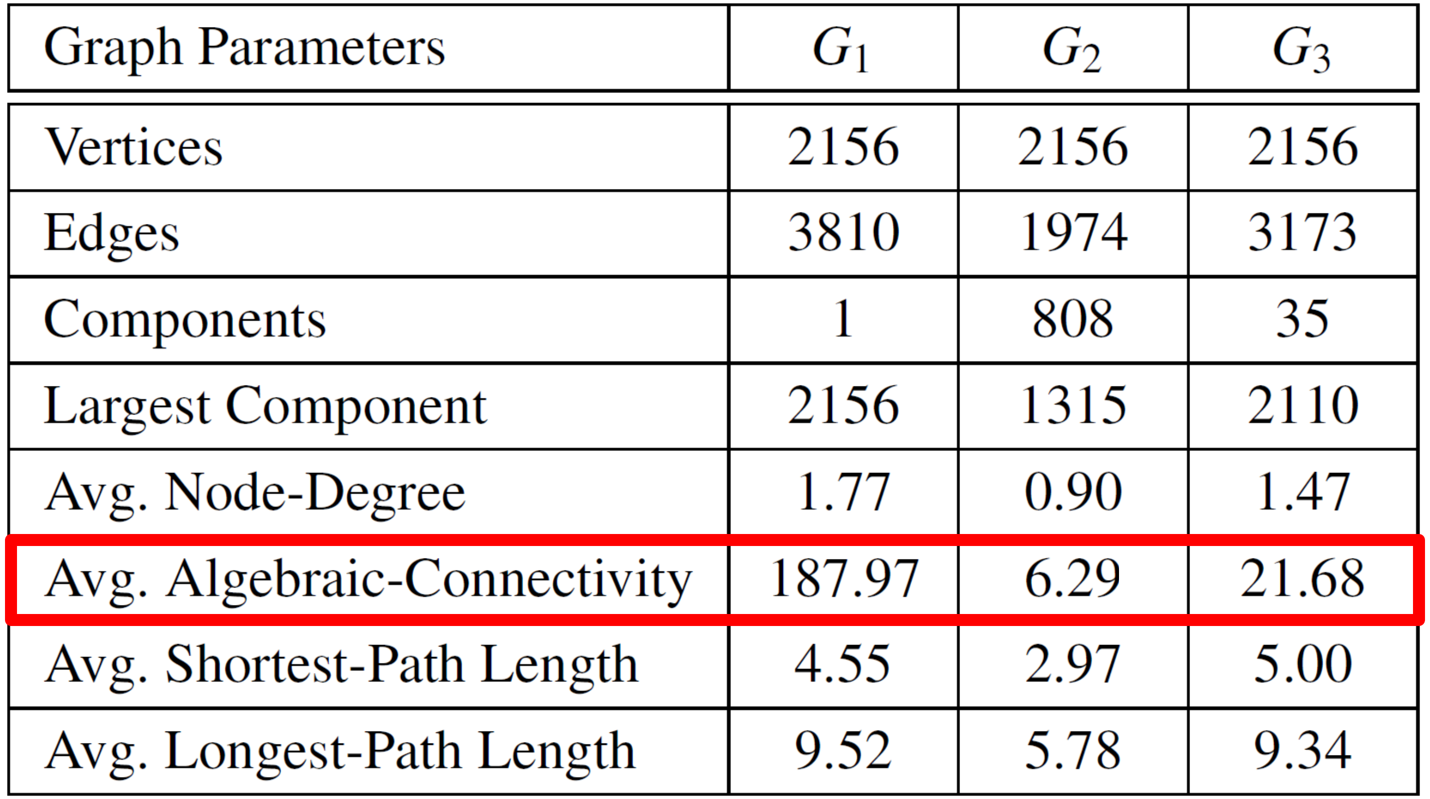
What is the Impact of ROV?



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

G1	G2	G3
No ROV	All ROV	IXP ROV

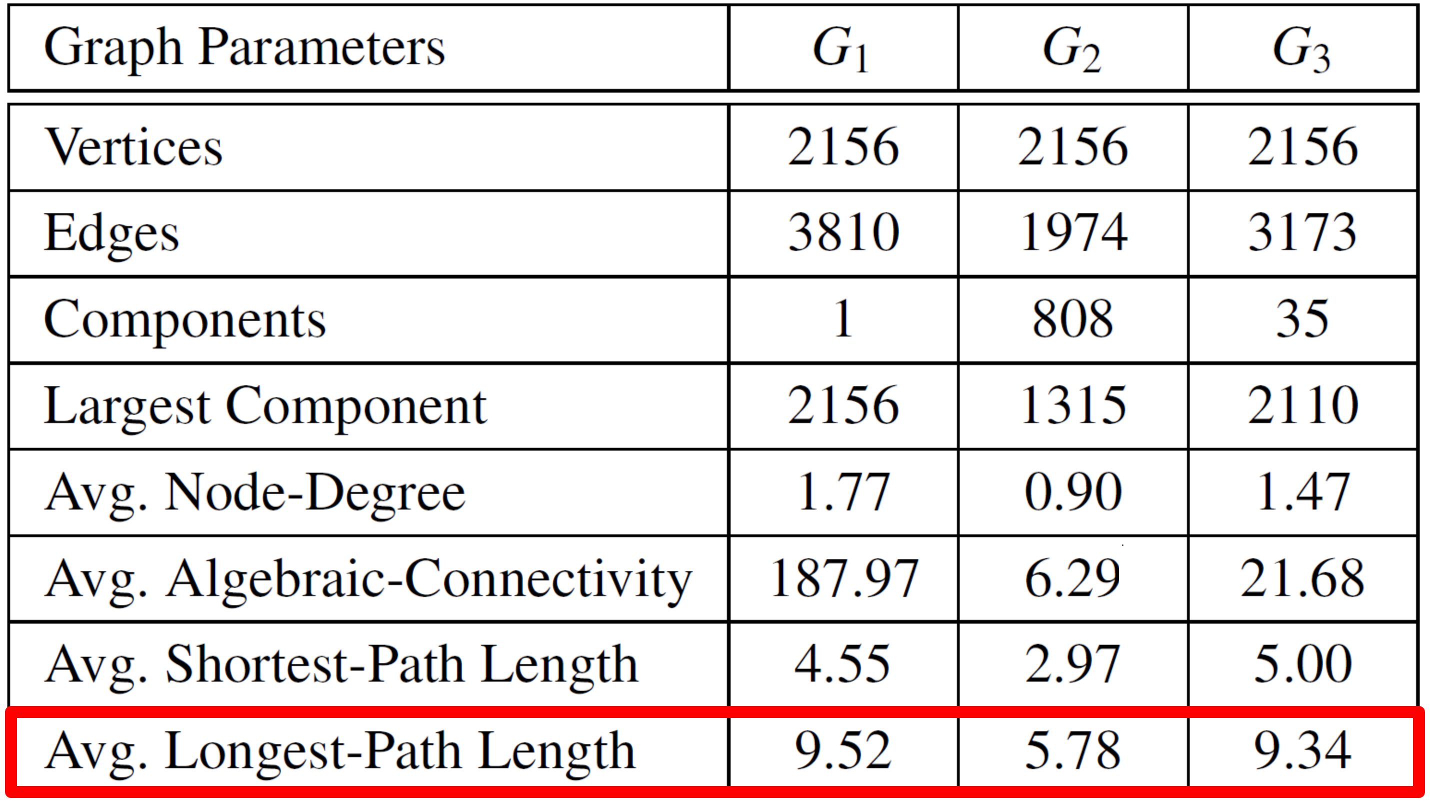
What is the Impact of ROV?



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

ROV reduces connectivity for hijacks

What is the Impact of ROV?



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

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

çok teşekkürler

תודה רבה!

谢谢

Merci beaucoup!

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございました

Dziękuję!

zor spas

Grazie mille!

اشكرك